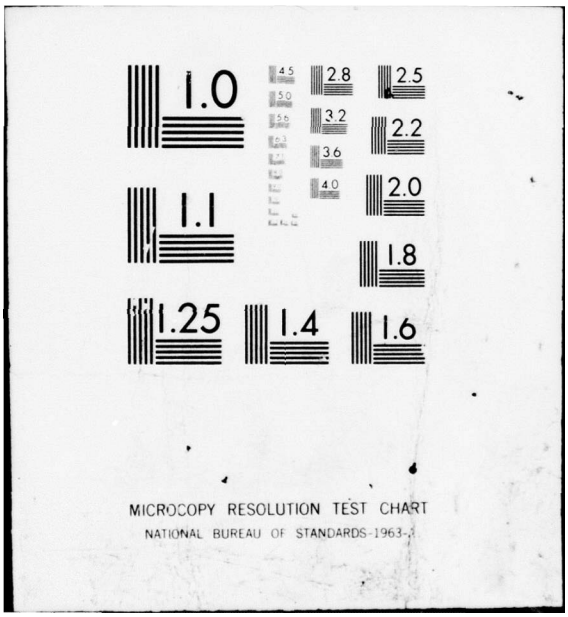
AD-A068 235 NATIONAL CLASSIFICATION MANAGEMENT SOCIETY ALEXANDRIA VA F/G 5/2
CLASSIFICATION MANAGEMENT. JOURNAL. VOLUME XIV, 1978,(U)
1978 J A ROBINSON

UNCLASSIFIED NL

1 OF 2
AD A068235


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

LEVEL II

CLASSIFICATION MANAGEMENT

C
M

JOURNAL of the NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME XIV - 1978

(6)

CLASSIFICATION MANAGEMENT.

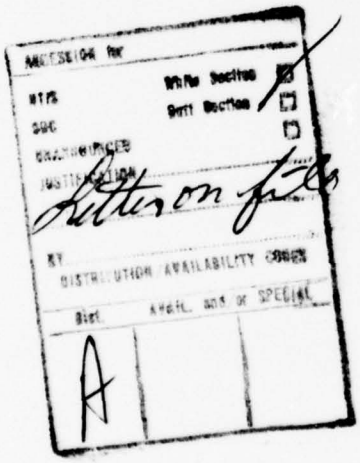
Journal.
Volume ~~XIV~~, 1978.

(11) 1978

(12) 131 p.

(10) Jack 1. Robinson

JOURNAL of the NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME XIV – 1978



Published by the National Classification Management Society. Mailing address: Executive Secretary NCMS, P.O. Box 7453, Alexandria, Virginia 22307. Director of Publications and Editor of this Volume, Jack A. Robinson. The information contained in this Journal presented by the several individuals, does not necessarily represent the views of the organizations they represent nor of the National Classification Management Society.

TABLE of CONTENTS

(over)

PART ONE

Proceedings of the FOURTEENTH ANNUAL SEMINAR 16 – 18 May 1978

Dunfey's Royal Coach Inn

Dallas, Texas

THE EVOLUTION OF THE 1978 EXECUTIVE ORDER, "NATIONAL SECURITY INFORMATION"

Dr. Robert M. Gates
National Security Council Staff

Introduction

It is a privilege – and no little challenge – for me to appear and speak about the new Executive Order on the classification system. I accepted the invitation to do so because *you* must implement the Order we have drafted.

We began the effort to revise the Executive Order nearly a year ago. A funny thing happened on my way to the Oval Office last summer with a fresh new Order – I ran into 26 Executive departments and agencies, the Domestic Staff, Office of Management and Budget, Bob Strauss, Special Representative for Trade Negotiations, Senators Muskie and Biden, Representative Preyer, the staffs of five Congressional Committees, the American Civil Liberties Union, Morton Halperin, *Access Reports,* The Gang of Four *and* the National Classification Management Society. Now you can appreciate what I really mean when I say I am pleased just to be here today. I am pleased to note that every government agency was a strong advocate of reform – of someone else's agency. It was a year of guerrilla warfare for and with the bureaucracy -- all to a "Greek Chorus" background of public interest groups chanting "Classify no more, classify no more."

Well, we survived the year and now, eleven major drafts later, the Order is on its way to the President. If he is content with what we have produced, it will become effective next winter.

Historical Background

Before describing to you what changes are in store, I think it would be useful to review briefly where we have been in this business of withholding information from the public – this business of security classification. Working with the details day after day, it is unavoidable that our perspective narrows and we lose sight of the place and problems of government secrecy in America.

As a recent paper by Richard L. Oborn details, secrecy has been a working tool of military affairs and diplomacy in America from colonial times.[1] During the War of the Revolution, General Washington invoked secrecy in his handling of intelligence sources and methods as he manipulated agents behind British lines. The members of the Continental Congress signed a secrecy agreement with respect to their proceedings – an agreement that certainly was upheld better than similar agreements in our own time. At the Constitutional Convention, the proceedings were conducted in complete secrecy and remained sealed for more than 30 years.

The first Executive restriction of information related to defense and foreign policy and came in 1790 when President Washington asserted the right to limit dissemination to the public under the Constitution. The first executive claim of secrecy was made in 1792 when the House asked Washington for materials related to an Indian massacre.

In these and other episodes, the practical and theoretical foundations were laid by President Washington for a claim to executive secrecy and the President's power to withhold certain information from the general public – and, on occasion, even from the Congress. There is a direct line from these early cases to the Post-war Executive Orders establishing our present classification system.

Until 1936, there was no formal classification system except for military information. All Orders or regulations up to that time were issued by the War Department or the Army and applied only to protection of military secrets – and rarely, foreign policy or diplomatic relations. In 1936, an Army regulation for the first time extended the category of protected information to include foreign policy material and "the interests or prestige of the Nation, an individual, or any government activity." They should try to sell that to Justice or the Hill today!

The use of classification to protect documents, not unexpectedly, burgeoned in World War II. The Office of War Information in 1942 issued government-wide security classification procedures, including controls on the identification, handling and dissemination of sensitive information.

At the end of the war, it was clear that while one menace to the United States had been defeated, another had emerged. To protect our vital atomic secrets from the Soviets, Congress in 1946 passed the Atomic Energy Act which, as later amended, created the first and only statutory protection.

---

[1] Thesis submitted to the faculty of the Graduate School of the University of Missouri, in partial fulfillment of the requirements for M.A. degree.

In the period since the war, there have been three major Executive Orders establishing and then reshaping the Government security classification system. For you to understand better the reasons for and significance of changes we are proposing to the President, I would like to review briefly some of the key provisions of these three Orders.

The Truman Order

The classification system as we know it came into being with President Truman's signature on September 24, 1951 of Executive Order 10290. He stated at that time:

> "... it is necessary, in order to protect the national security of the United States, to establish a system for the safeguarding of official information the unauthorized disclosure of which would or could harm, tend to impair, or otherwise threaten the security of the nation. ... it is desirable and proper that minimum standards for procedures designed to protect the national security against such unauthorized disclosure be uniformly applicable to all departments and agencies of the executive branch of the government and be known to and understood by those who deal with the Federal Government ..."

For the first time, then, the security classification system was consolidated and extended to all executive agencies. The key elements of the Order included:

- A four tiered system using the designation Top Secret, Secret, Confidential and Restricted. The type of information in any of the four categories was vaguely defined and open to interpretation.

- No limits were placed on the number of classifying officials. Information could be classified by an "appropriate classifying authority," a term that was undefined. The power of agency heads to delegate classification authority was unlimited.

- There was no provision at all for automatic declassification, although an optional procedure was offered that called for the classifier to note on the document a date or event, passage of which would free the material for automatic downgrading or declassification. The Order specified *constant* review to determine when documents should be declassified but no implementing procedure was adopted.

The Truman Order was widely denounced by the news media and the Congress, who charged that the new system would allow the government to cover up mistakes and political intrigues while allowing official leaks.

The Eisenhower Order

Dwight Eisenhower ran for President promising to conduct an open government. Once elected, he responded to criticism of the Truman Order with a new Order of his own revising the classification system. The White House introduced the Order with the following words, which have come to have a familiar ring:

> "Throughout the lengthy consideration of this Order it has been the purpose to attain in it the proper balance between the need to protect information important to the defense of the United States and the need for citizens of this democracy to know what their government is doing."

Executive Order 10501 with its amendments, had the following major provisions:

- It limited the classification designators to Top Secret, Secret and Confidential (eliminating restricted)

- For the first time, serious attention was given to declassification. Heads of agencies were required to designate someone to be responsible for review of information for declassification and receive requests for such review "from all sources." Material was to be organized into four groups – foreign government, atomic energy, intelligence and cryptographic information, which were entirely exempt from declassification; extremely sensitive information designated by an agency head or his designees, which was entirely exempt; information warranting some degree of classification indefinitely, which was to be downgraded every 12 years until it was Confidential, where it would remain indefinitely; and information not in those three groups, which would be downgraded every 3 years until confidential and then automatically

declassified 12 years after issuance. Automatic declassification remained non-mandatory, *i.e.*, no date such as 30 years was established.

- For the first time, the Order stated that the President would designate a member of his staff to receive and take action upon suggestions or complaints from non-governmental sources relating to the Order. Further, the NSC was directed to conduct a continuing review of implementation of the Order to ensure that classified defense information would be properly classified.

The 1953 Order, with its amendments through 1967, stimulated declassification on a systematic basis and made a number of changes designed to limit the number of classifiers, fix responsibility for classification and speed the release of classified historical information.

The Nixon Order

In January 1971, President Nixon formed an interagency committee chaired by the Assistant Attorney General William Rehnquist to review classification procedures. The project moved slowly, however, until release of the Pentagon Papers. The Committee met with the President on July 1 of that year and then worked through the summer and fall on a draft Order, which was circulated to the agencies in January 1972. Executive Order 11652 was signed on March 8 and, as you will remember, became effective on 1 June. Let me mention the principal changes it directed in the system. The Order:

- Reduced the number of departments and agencies authorized to classify
- Restricted classification authority delegation;
- Accelerated the downgrading and declassification schedule; automatic declassification after 6-10 years excluding exemptions (limited to four specific categories of information); and provided for mandatory review after 10 years for exempted documents
- Provided declassification of classified information after 30 years unless an agency head specifically continued protection
- Gave the National Archives the duty of reviewing and declassifying information classified under previous Executive Orders and more than 30 years old
- Allowed administrative sanctions against those who abuse the system
- Established an implementation and classification review body – the Interagency Classification Review Committee.

The Order encountered considerable criticism, especially from the Congress. It was characterized as "a shoddy technical effort with major deficiencies." The then Foreign Operations and Government Information Subcommittee even issued a report solely on the defects of the new Order.

Despite the comments of detractors, EO 11652 was a progressive Order that tightened rules for classification, opened the way to much greater declassification of previously protected government information, created an oversight body, and significantly reduced the number of authorized classifiers. With regard to the last change, in view of criticism in 1972 that the Order would result in more classifiers, the number of authorized classifiers dropped 78 percent between early 1972 and today – from 59,000 to just 13,000. Today, under this Order, in a Federal establishment of over 6,000,000 people – more than half in the Defense Department – there are fewer than 1400 officials authorized to classify Top Secret. No matter how you slice it, that is an important improvement.

Nonetheless, experience with EO 11652 demonstrated that further improvements were needed and were possible to promote openness as well as better protect that information needing protection. Implementation of EO 11652 was a learning process precisely because many of its policies and requirements were a significant departure from those of the Eisenhower Order which it replaced. The major lessons learned bear mention in view of their influence on the new draft and I shall cover them.

The classification crisis under Executive Order 10501 stemmed in part from deficiencies in the implementation and enforcement of its provisions. Executive Order 11652 sought to deal with this problem by establishing monitoring and review functions under the Interagency Classification Review Committee. But, while the establishment of an oversight body had a positive effect on departmental programs, ICRC responsibilities and powers were vaguely worded in the Order and, because they were not explicitly binding on

the agencies, could safely be ignored. It had little authority to require agencies to open sensitive files to inspection or to submit regulations for review; to declassify agency documents classified in violation of the Order; to issue directives for implementation of the Order; and lacked other powers necessary to make it an effective oversight body. Further, a significant proportion of the ICRC's time and staff were assigned to processing appeals of agency declassification decisions. This work, together with various training activities, severely curtailed the ICRC's capability to serve as an effective oversight body.

The incorporation in the Order of four broad categories of exemptions from the general declassification schedule was overused and contributed to material being provided security protection far longer than its sensitivity warranted. This was compounded by permissive language of the Order which required the setting of a date or event for declassification "unless impossible to determine." Experience showed that the exemption was extensively used, thereby resulting in considerable information being placed in a status whereby classification will continue without necessary review, for a full 30 years. In fact, over half of all classified material was exempted from the general declassification schedule. Failure of the Order to include specific restrictions and accountability with respect to the duplication of classified documents left the way open in the 1970's to even more massive copying and greater loss of control of information by originating agencies. Inconsistencies between the Order and the FOIA led to the perpetuation of a dual declassification system in most agencies that was confusing to the public and an administrative burden to the Executive Branch. The sometimes permissive and vague language of the Order was often an impediment to uniform implementation. The use of terms such as "whenever possible" rather than "shall" or "will" encouraged some departments to regard their responsibilities towards implementation of certain aspects of the Order as *voluntary* rather than *mandatory,* and further weakened the ability of the ICRC to exercise its authority as an oversight body. The Order did not mandate the identification of the level of classification of portions of classified material. The lack of such a requirement often resulted in the unnecessary classification or overclassification of material marked on a derivative basis.

The Carter Order

For the past 20 minutes, I have force-marched you through the history of security classification from Biblical times to the present. Our current system retains many features from the past, some worthwhile, some not so worthwhile. But an unmistakable feature since 1953 has been a steady effort to impose tighter controls on the classification process and to hasten and broaden the declassification of no longer sensitive national security information. That effort would be continued and accelerated by President Carter.

Throughout his long campaign for the Presidency, Jimmy Carter expressed his commitment to making the policy-making process more open to the American people; to making more information available to Americans so they could observe and participate more directly in the making of decisions that affect their lives. Thus, early in 1977, the President asked Zbigniew Brzezinski and Stuart Eizenstat, his advisors for foreign and domestic affairs, to look into further reform of the security classification system. A joint NSC-Domestic Staff Committee was established in June and instructed to consider:

- How to provide for the maximum release of information to the American public on government activities and policies consistent with the need to protect sensitive national security information;
- How to promote increased public access through a more rapid and systematic declassification program;
- Overlaps between the new Executive Order and the Freedom of Information Act (FOIA) as amended and the Privacy Act;
- Which information requires protection and for how long;
- Which categories of classified information or material more than 20 years old could be declassified in bulk under appropriate guidelines;
- How the classification system can be simplified;
- How to eliminate unnecessary and duplicative practices
- Whether Departments and Agencies should prepare classification and declassification guidelines;

- What kinds of disciplinary actions can be taken to prevent the misuse of the security classification system by government officials;

- How best to implement the provisions of the new Executive Order.

I should add that, on our recommendation, the President directed that the new Order be ready for his signature by September 15. How, given the experience of our predecessors, we ever dreamed we could fundamentally reform the system in that limited time escapes me. There has not been such a display of hubris by officials of the government since Custer camped at the Little Big Horn. I might add that the consequences were similar.

We truly wished to explore all possibilities for seriously revamping the system. Working groups were established to develop far-reaching options for changing all aspects of E.O. 11652. We devoured the works of Mr. Halperin and other students and critics of the system; we consulted with staff members of several Congressional committees and solicited their ideas for change; we spoke often to representatives of this organization; and not least, many of you as individuals offered suggestions. Advocates of broad reform from OMB, Justice, the White House Domestic Staff, the ICRC and National Archives participated in the working groups together with representatives of the Departments of Defense, State, CIA and other agencies – who themselves brought many ideas for change based on past experience.

I cannot tell you how gratifying it was to see the Department of Defense pressing day in, day out, for tighter controls on classification and improved declassification – at CIA; to see State doing the same – to Defense; to see CIA playing honest broker – until there was a move to force declassification of all intelligence materials at 20 years; and over them all, pure of heart and sage of mind, the Justice Department – that is, until the roll of the dice brought FBI procedures up for review.

Seriously, I was astonished at the cooperative spirit and genuine interest in constructive, workable reform demonstrated by all the participants. As examples, CIA and Defense were the foremost advocates of including for the first time, restrictions on programs for special compartmented information; all agencies supported the move to 20 year systematic review; all supported restrictions on *post hoc* classification after an FOIA request is received; nearly all endorsed paragraph marking; all accepted the idea of a balancing test; and all enthusiastically supported creation of a strong Oversight Office.

A draft Order was submitted to the agencies – and for the first time, to Committees of the Congress and interested members of the public – for comment in September. The response was a nearly unanimous bronx cheer – from inside and outside the Executive branch. Over 500 specific points were addressed in comments on the draft. While a few likened us to Attila the Hun and suggested that the draft was an effort worthy of the staff of Millard Fillmore, most of the comments were very constructive. And so began the arduous task of reshaping the draft to meet the criticisms of liberals and conservatives, classifiers and non-classifiers, the critics and advocates of secrecy. Thoroughly objectionable sections, such as that on secrecy agreements – which incidentally only ratified present arrangements – were deleted; others were modified to overcome clear shortcomings. Overall, some 75 percent of the comments resulted in changes to the draft.

A second draft was issued in late December. The reaction was much more favorable, but made clear that important internal executive branch disagreements existed and that a major effort also lay ahead to translate the draft into English and to refine it. This process continued through the winter and early spring. Congressional staff views were sought again and resulted in further changes, for example in the classification criteria – which were completely redrafted and abbreviated. Negotiations on the language of the balancing test, the two stage classification process, the nature of the Oversight Office and other issues stretched on for weeks and even months.

I am pleased – and you will never really know how pleased – to tell you that last week the eleventh major reddraft of the Order was sent to OMB for final processing to the President.

You have patiently borne the burden of listening to a bureaucrat recount in excruciating, if not soporific, detail the history of a particularly arcane art form – the classification of government documents. You have passed this trial by fire and can now permit the glaze which descended over your eyes some minutes ago to recede. For the benefit of the survivors, I would like now to review the principal changes and new features in the draft Executive Order.

Classification Process

1. Under the old system, a document could be classified if its release would damage national security. Under the new Order, two tests must be met:

- Information may not even be considered for classification unless it falls within one of 6 classification criteria. The "seed catalogue" of 13 criteria in earlier drafts has been cut in half. An agency head may classify categories of national security information outside those six areas, but must inform the Oversight Office of his decision; and

- There must be reasonable expectation that unauthorized disclosure of the information will cause identifiable damage to the national security.

These changes are intended to make classifiers' decisions more thoughtful and less automatic. They should help prevent unnecessary classification. Further, the new classification criteria are limited to information on defense and foreign relations. This listing of criteria is intended in part to affirm that information about domestic affairs may not be classified.

2. The new Order requires that most documents be classified section-by-section, not as a whole The new procedure will allow ready identification and release of the unclassified parts of classified documents.

3. There are five new prohibitions against classification, which are now centrally located in the Order.

4. The new Order will reduce the number of agencies authorized to classify information. It strips 10 agencies of classification authority and reduces the authority of several others.

Duration of Classification

5. The new Order sharply cuts the duration of classification.

Under the old system, most information was covered by the General Declassification Schedule (GDS). Documents were automatically declassified in six to ten years, depending on whether the information was Confidential, Secret, or Top Secret. Officials with Top Secret classification authority exempted substantial numbers of documents from this system. (In theory, such exemptions were limited to four categories, but the categories were drawn so broadly they were ineffective, and were often disregarded altogether.) Documents exempted from GDS would stay classified until they were 30 years old, when they would be reviewed and – with some exceptions – declassified.

The new system abolishes GDS and makes the duration of classification depend on the content of the information, not its classification level. Under the new system, most information will be declassified after *no more than six years.* Officials with Top Secret authority can set longer terms, but they must provide specific justification. In another significant change, the documents which are given longer terms will now be reviewed for declassification *after 20* years. The switch from 30 to 20 years will be phased in gradually, and will result in the release of over 600 million pages of formerly classified information.

Declassification Process

6. For the first time, the declassification process will include a so-called "balancing test." That means that in appropriate cases the public's interest in knowing the information is to be balanced against the need to keep it classified. When the interest in disclosure is greater, the information will be released, even though its continued classification could be justified.

7. The new Order requires agencies to declassify information as early as national security permits and to give declassificaton as high a priority as classification. In addition, the number of officials authorized to declassify information will be increased.

8. The new Order has been generally conformed to the FOIA with respect to declassification requests. All non-Presidential information will be subject to request for declassification regardless of how long it has been classified.

9. The new Order will require heads of agencies to prepare and promulgate declassification guidelines applicable to information as it becomes 20 years old. Information falling outside these guidelines will be automatically declassified at 20 years.

Other Changes

10. The new Order creates an Information Security Oversight Office to police the classification system. The Office will have enumerated, specific powers, including authority to inspect agencies' files and procedures and to challenge such procedures as well as

agency classification decisions. The Office will be located in the General Services Administration, under the supervision of the National Security Council.

11. The new Order will allow the continued use of compartments – they are needed for especially sensitive information – but will reduce their number. Henceforth, compartments may be created only upon a written finding of necessity by an agency head. A "sunset" provision will terminate each compartment after five years unless a new finding of need is made.

12. The new Order requires agencies to impose administrative penalties for unnecessary or excessive classification and creates procedures to assure that violations of law are reported to the Justice Department.

13. The new Order for the first time imposes specific administrative restrictions on copying classified documents.

14. The new Order says that classification may not be restored to documents once they are officially released to the public.

15. Agencies will be required to prepare classification guides to facilitate the identification and uniform classification of information requiring protection.

16. A number of technical changes have been made in the Order, the overall effect of which is to weight the Order in favor of greater openness and against unnecessary classification.

CONCLUDING OBSERVATIONS

If the three preceding Orders are any guide, we can expect criticism of the Carter Executive Order for not going far enough or for going too far; as a document written by classifiers for classifiers; for failing significantly to reduce the number of classifiers; for applying an explicit balancing test only at the time of declassification; for failing to put an end to compartments; for drawing the classification criteria so broadly, and so on.

This is my answer. This Order, as those that preceded it, is the product of compromises – between those who classify and those who don't; between ideal solutions and workable remedies; between Executive prerogatives and responsibilities on the one hand, and Congressional and public interest pressures on the other. I believe that, despite some of these compromises and perhaps because of others, the Administration has produced a good draft Executive Order. It marks an important step forward in the continuing process of redefining the balance between the public's right to know and the need even of a popular government to protect certain matters concerning defense and foreign relations.

My perhaps overlong review of the historical background of this Order has been intended to underscore that the new Order is part of an evolutionary process toward greater openness. The Order is not revolutionary; Washington will not be littered after December 1st with broken bureaucratic crockery. But no fair-minded person can deny that the Order responsibly moves the Executive Branch toward greater public access and more scrupulous adherence to workable but restrictive rules for classification and extended protection. Such change is lasting change. This Order builds on its predecessors as someday it too will serve as the foundation for further change.

Today, no government in the world permits its citizens such ready access to its inner councils and to its defense, diplomatic and intelligence affairs. With this new Order, that gap will be further widened. That broad access, and the public's insistence and trust that government act responsibly when it must deny such access, jointly strengthen this country. You, who are responsible in and out of government for managing the security classification system, are the custodians of that public access and public trust. If you fail to uphold and encourage public access – as has happened in the past – public trust will falter; if you fail to protect our legitimate secrets – as has happened in the past – our national security may be damaged. While you may at times consider your work routine and bureaucratic, in truth you bear heavy responsibility both for maintaining trust in our government and for our national security. Your faithful and conscientious fulfillment of this responsibility now and after December 1st will bring the new Executive Order to life and ensure that its provisions enhance both trust and security – with a stronger America the result. Be assured that in meeting this challenge, you and the new Oversight Office will have the full support of the National Security Council.

DOD PLANS FOR IMPLEMENTING A NEW EXECUTIVE ORDER

David O. Cooke
Deputy Assistant Secretary of Defense (Administration)

It is a pleasure to have this opportunity to discuss the Department of Defense plans for implementation of the new Executive Order on the security classification system.

As Dr. Gates established, it has been a long road since President Carter signed PRM-29 on June 1, 1977 and directed revision of Executive Order 11652. We in the Department of Defense fully support the objectives of the President in undertaking the revision of the present Executive Order. We have worked hard in developing the new Executive Order and believe that it will lead to further improvement. Now that most of the hard rowing necessary to develop the new Executive Order is behind us, there may be a tendency to rest on our oars, which of course, would be a dangerous thing to do. Switching metaphors, the new order is only a skeleton; to achieve the President's objectives we must provide the operating flesh by effectively implementing its policies throughout the Executive Branch and its contractor facilities. In no other Department is the challenge of implementation so great as in Defense. The Department has about three million people located at about eleven-hundred activities worldwide who are responsible for great numbers of classified documents. Further, the Department has the primary responsibility for the Defense Industrial Security Program. Let me assure you that we intend to fully meet the challenge of effective implementation.

We are confident, and you may wonder why, of being able to meet the challenge. Consider for a moment that the Department's regulation that implements Executive Order 11652 foreshadowed some of the provisions of the new Executive Order. For example, the regulation contains classification criteria, one of the key and distinguishing features of the new Executive Order. A further requirement of the regulation, as in the case of the new order, is that information falling within the criteria may not be classified unless a determination is made that the unauthorized disclosure of the information could reasonably be expected to cause a degree of harm to the national security. Paragraph classification marking has been mandatory within the Department since 1964; the draft Executive Order would extend this requirement to the rest of the Executive Branch. The Department's implementing regulation also covers another point of the new Executive Order – the "balancing test" – which is expressed in the regulation in a way calculated to stimulate the thought process of the classifier by keeping the public's need for information regarding the affairs of government in the classification picture. And, of course, the Department's regulation already treats the subject of classification guides in some detail and it would appear that classification guides will be required of everyone under the terms of the new order.

We are confident of meeting the challenge that lies ahead for other reasons as well. Since Executive Order 11652 became effective, the Department's massive security training program has built up a considerable reservoir of talent which will be essential to the successful implementation of the new Executive Order. We have been educating Defense people to understand that security classification is to be continued for the shortest time possible consistent with the interests of national security. Such training should pay off in view of the new Order's shorter time limits for the duration of classification. And, of course, we plan to continue our monitorship efforts through program reviews at all levels of Defense and Defense industry. The fact of the matter is that over the past several years the Department has been continuously refining its policies, practices and procedures to achieve a more viable Information Security Program and, it appears, a more viable Executive Order.

I wish to point out here that we are well aware of our responsibility to follow the provisions of the new Order. We are also aware of their impact on Defense operations and have already initiated actions to gear up for effective implementation. When the new Executive Order is signed, we plan to circulate within the Department a draft of the new DoD Directive which will be formally coordinated with some thirty DoD Components and offices. This coordination effort should begin almost immediately after the new Executive Order is signed as the DoD Directive has been in draft form for some time now; only some last minute adjustments will be required to conform it to the new Order. Further, it should be only a few pages long as it will be only the basic charter for the Information Security Program within the Department.

Next, let's look at how Defense implemented the details of Executive Order 10501, the predecessor to the current Executive Order 11652. Under the old Order, we had what may be characterized as a master security program Directive and other DoD Directives

and Instructions providing Defense-wide implementing details. Those DoD Directives and Instructions were, as today, issued by the Office of the Secretary of Defense. All required extensive implementations by each of the Military Departments and Defense Agencies in order to adapt the fundamental policy to the diverse requirements and organizational structures of the DoD Components.

Then, to implement Executive Order 11652, it was decided to try a new approach. A single DoD Directive was issued to charter the Information Security Program. That Directive spelled out basic responsibilities and set out the authorization for a single Defense-wide regulation – the Information Security Program Regulation. The Regulation was issued at the OSD level without a requirement for further formal issuance by any DoD Component though the Components were authorized to issue the necessary supplementary instructions to provide for the internal administration of the Regulation. As compared to the first method of implementation, the current Defense implementation has certain advantages, including:

- Less lead time is required for publication as the necessity of successive and multiple coordination efforts is avoided.
- More uniformity of procedures among the several Defense Components is realized, no doubt increasing efficiency.
- A common point of reference is established, thus facilitating communications among Defense Components.

Finally, in anticipation of implementing the forthcoming new Executive Order, both approaches were given new consideration; the advantages and disadvantages of each were weighed again. Last November, our Director of Information Security, Mr. Van Cook, sent two of his people out on a round-robbin of informal visits to the three Military Departments, the Organization of the Joint Chiefs of Staff, and key Defense agencies like the Defense Intelligence Agency and the Defense Nuclear Agency. During the visit his people, among other things, obtained candid views on the merits of both methods of implementing the new Executive Order. Almost without exception, the Defense components were strongly in favor of the current setup, that is, a single DoD Directive and a single DoD-wide regulation not requiring Defense Component implementation but one which would continue the practice of authorizing supplements for the purpose of providing for the internal administration of the Regulation. So we've decided to continue the single regulation concept within the Department. I don't mind telling you that the results of the straw-vote taken earlier had a bearing on the decision. After all, there is a degree of democracy in the management of the Department's Information Security Program.

Some of you will recall the massive team effort required to get out the first edition of the Department's Information Security Program Regulation in 1972. Many people said that it could not be done in the two weeks available for the job. But it was done in time – between May 17, 1972 when the National Security Council's Directive was issued and June 1, 1972, the effective date of Executive Order 11652. As an *ad hoc* committee is already at work on the new National Security Council directive, we anticipate an adequate amount of time for the task of writing a new Regulation but we still figure on a team effort. Again, we hope to get the experts from the Military Departments involved with the drafting of the new Regulation and, circumstances permitting, we may seek the help of a few industry experts as well because, as you know, the policy established in the Department's Information Security Program Regulation finds its way into the Industrial Security Manual to one extent or another. This way, we'll have the major inputs incorporated in the draft Regulation prior to its being entered into the formal DoD coordination system. To get the biggest possible head start on the job, Art Van Cook's crew has been looking at the existing Regulation in light of the provisions of the forthcoming Executive Order. The need for many changes to the Regulation has been identified, however much remains to be done.

Full implementation of the new Executive Order within Defense depends upon more than just the DoD Directive and Regulation. For example, one of the provisions of the new Order will require that agency heads ensure the preparation and promulgation of guidelines for security classification that will facilitate the identification and uniform classification of information requiring protection under the provisions of the Order. Accordingly, we are about ready to begin formal coordination of a draft DoD Handbook for Writing and Applying Security Classification Guidance. It is our intention to complete the coordination process for this Handbook in time to have it on the street before the effective date of the new Order. By doing so we should be in a good position to help assure timely revision of the more than 800 security classification guides currently in force within the Department of Defense.

It is important to keep in mind here that the coordination drafts of the DoD Directive, Regulation and Handbook will all pass through the same activities and offices in Defense within a short time frame and thereby add a considerable workload to every-day business. Accordingly, we are making every effort to get as much of the work done ahead of time as possible. We hope that will facilitate the coordination process by turning out a better product at the start – one that should be easier to review and comment on.

I've already mentioned another publication that will require substantial change to conform to the provisions of the new Executive Order – the Industrial Security Manual. Though much of the work on the manual is done by Colonel Pruett's office at the Defense Logistics Agency's headquarters, its impact extends far beyond the Department of Defense to sixteen departments and agencies outside of the Defense establishment and to the thousands of contractors engaged in the Defense Industrial Security Program. As you may know by now, the terms of the proposed Order will, among other things, change and simplify classification and declassification marking requirements. Thus, there will be a need to revamp certain parts of the Industrial Security Manual. Our intention is to accomplish these and any other necessary changes just as soon as possible so that you in industry will have an Industrial Security Manual compatible with the provisions of the new Executive Order and its implementing directives. The Council of Defense and Space Industry Associations will, of course, have the opportunity to review and comment on any revision of the Manual prior to publication. We are, as you can see, endeavoring to make the transition from the current to the new Executive Order just as smooth and timely as is possible.

Another important facet of the Department's plans for implementation of the new Order concerns the Order's proposed and almost certain requirement that agency heads of the Executive Branch issue guidelines applicable to twenty-year old information. Such guidelines will have to be issued not later than 180 days after the effective date of the new Executive Order and will address limited categories of information that should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond twenty years is required. Thus, within Defense, you could have four sets of guidelines – one promulgated by the Secretary of Defense and one each by the three Military Department secretaries. Or, on the other hand, we could opt for a single set of guidelines applicable to the entire Defense establishment. Right now we are leaning toward a single set of twenty-year guidelines on the basis that our current declassification guidelines for pre-1946 and pre-1950 information and material seem to work well. In these guidelines, the Deputy Secretary of Defense has stated in effect that all DoD information classified on or before June 30, 1950 is declassified with the exception of several narrowly defined categories such as cryptology. I might add here that a good deal of effort has already gone into the task of updating the existing guidelines to fit the requirements of the new Executive Order so that we can stay a jump ahead of things in the future.

As many of you are aware, we in the Department of Defense have been actively engaged in monitoring the Information Security Program within the Department and in Defense industry. One of the primary ways we keep tabs on things is through our Program Reviews. We will, of course, continue these Reviews under the new Order as they are quite effective. Just as soon as the new Executive Order is signed we will change the character of our Program Reviews from the normal inspection and education format so that we can spend more time on the educational aspect – education of the people who will have to thoroughly understand the workings of the new Order to make its implementation efficient and effective. In this connection, Mr. Van Cook has already advised me of his intention to get his people out early for the purpose of familiarizing defense and industry personnel with the provisions of the new Executive Order. After that has been accomplished, we'll resume the normal conduct of Information Security Program Reviews.

Though changed in some respects, the new Order will continue the mandatory declassification review system first set up under Executive Order 11652 and will require that agency heads establish a process to decide appeals from denials of such declassification requests. In connection with appeals, I should point out that the new Executive Order will abolish the Interagency Classification Review Committee and replace it with an Information Security Oversight Office. The Director of the new Office will hear only those appeals which involve "Presidential records."

Based on the draft requirements of the new Executive Order, we will be taking renewed action to ensure that there is a demonstrated need for access to classified information before a security clearance application is filled out. The continued need of people who are granted access to classified information will be scrutinized with the objective of holding the number

of cleared people down to the minimum consistent with operational requirements. We will also be renewing our effort to ensure that safeguarding practices are reviewed continuously and to ensure elimination of those that are found to be duplicative or unnecessary.

All of this is a tall order to be filled in a relatively short period of time between signing of the new Executive Order and its effective date. However, the way things look now, there will be a sufficient amount of time available for an orderly implementation process. Adequate time for the task is essential when one considers the complexities and magnitude of the job within the Department of Defense and in Defense industry. I believe that gives you a fair idea of our plans for implementation of the forthcoming Executive Order. As I have indicated, we will be consulting with you just as much as is possible in the days ahead.

In the last analysis the successful attainment of the President's objectives depends not on the new Executive Order and implementing regulations but on people – people like the members of the Society. I will be looking forward to the continued cooperation of the Society. We have worked well together in the past and must do so in the future to help assure the well-being of our national security interest. I am confident that the new Executive Order will serve *that* interest admirably and *also* provide a greater degree of openness in government.

MONITORSHIP

The Role of the New Information Security Oversight Office

Robert W. Wells
Executive Director, Interagency Classification Review Committee

Introduction

I welcome the opportunity once again to address this society and discuss some aspects of and share my personal views on the Information Security program. During the past few years I have come to know many members and to appreciate the unique as well as the mutual problems which are found among them. Moreover, I have come to appreciate the professionalism of the members and have from time to time, called upon individual members and your Board of Directors to provide background or other information which the Interagency Classification Review Committe needed to help improve the overall program. I thank you for your cooperation in the past and look forward to your further contributions.

Turning then to the subject – *Monitorship, Past and Future*. It is singularly appropriate to discuss this at this time in view of the expanded emphasis on that function found in the draft of the new Executive Order. As established by Dr. Gates previously, the Order has not yet been signed, the implementing directive is in only very rough draft form, and there is no indication of who will be appointed as the director of the new Information Security Oversight Office created by the Order. It would be true to say that under these circumstances I am in need of a well-polished crystal ball to focus the diffused outlines of the shape of things to come. So, to emphasize, much of the content of my presentation will be based upon my own personal experiences; how I think the new Oversight Office should be organized, how it should operate, and what additional changes I feel are needed to achieve a more effective oversight of the Information Security Program. My personal views may or may not coincide with those of the person selected to be the new director. Yet, in my view, there is merit in such a presentation because the topics will be presented from the vantage point of an Executive Director of the ICRC. There is considerable change ahead in the oversight function, but the new Oversight Office will, perforce, evolve from the present interagency committee.

The Present in Perspective

Let's take just a few minutes to look at the monitorship program under the present Order – Executive Order 11652. Under it, agencies granted original classification authority were required to appoint a central figure who would be in charge of overall monitorship and implementation of the Order. Moreover, they were charged with the responsibility for establishing monitorship programs and reporting to the ICRC data required by it as surveiller of program progress. The subject of progress will be covered later. The Interagency Classification Review Committee was a new idea at the time of EO 11652. It was the first time a White House level oversight body had been established to provide a measure of enforcement for the Government's Information Security Program. As you will recall, it is composed of senior representatives of the Departments of State, Defense, Justice, Energy, the CIA, the National Security Council Staff and the Archivist of the United States. The committee began its operations in 1972 under the chairmanship of John

Eisenhower who continued in that capacity until April 1973 when Dr. James B. Rhoads, the Archivist of the United States, was appointed as the Acting Chairman.

In the earliest days, the *entire* committee staff consisted of an Executive Director, and from time to time, two administrative personnel. The staff and the office was physically located in the Old Executive Office Building and the Executive Director was a member of the White House staff. Shortly thereafter, responsibility for supervision of the staff was shifted to the Office of Management and Budget and, when Dr. Rhoads was appointed as Acting Chairman, the staff and offices were placed in the National Archives for administrative support. It was argued at that time by the committee that moving the staff and office from the White House complex would have a detrimental effect on the committee and its work as well as on the effectiveness of the Executive Director in his relationships with executive branch departments. In September 1974, the committee forwarded to the Assistant to the President for National Security Affairs recommendations that:

- A permanent chairman of national stature be appointed
- The President, in connection with the appointment, make a strong public statement in support of the committee and its work
- Oversight of the committee's work be returned to the Executive Office of the President and that the staff be moved back
- The size of the staff be increased.

The committee advised that the National Security Advisor considered the return of the office to the White House complex "desirable," but despite repeated efforts by two executive directors, including me, the move never came about. Some modest progress *was* made in increasing the size of the staff. Approvals in 1975 and 1976 increased the staff, to a current eight – the executive director, four program analysts and three administrative persons.

Because of staff limitations, monitorship of the committee during the early days of its operation was limited strictly to review of the various reports required of agencies; *i.e.,* reports on classification authorities, abuses, unauthorized disclosures, requests for declassification review, appeals, and a quarterly summary report on classification actions and declassification determinations. With the increase in the size of the staff, I was able to institute a comprehensive system of what we call "program reviews" – by another name, "inspections". In 1976 the staff conducted 48 such reviews and in 1977 increased this by 100% to 96. As you might imagine, the reviews have become the "bread-and-butter" of our monitorship program.

In addition to six recurring statistical reports, the ICRC required departments to submit on an annual basis narrative evaluations of the progress they had achieved in implementation of the order. These evaluations covered areas such as education and training; the establishment of programs for systematic declassification review and similar items. On-site program reviews were one of the most effective means of ensuring implementation. Through such actions the committee acquired a first-hand look at personnel, organization, policies and procedures within the various departments. Moreover, they provided the ICRC with an insight into problems faced by agencies in implementing the order and identified areas wherein greater oversight emphasis was needed or change was required.

What then, in general, has been achieved over these last few years in the program?

- There is an increased awareness on the part of executive branch employees regarding the policies and the intent of the Executive Order – particularly the basic policy that the interests of the United States and its citizens are best served by making information regarding the affairs of government readily available to the public. This awareness may be due in part to increased coverage in the press over the last few years regarding classification and the release of classified information. Most certainly the Freedom of Information Act, which actually puts a person on guard to be able to defend his classification decision in Federal Court, has had an impact. Equally, the increased awareness stems from managements' interest and from good security orientation programs.
- There has been a steady decrease in the number of officials with original classification authority since promulgation of Executive Order 11652, though, not surprisingly, the rate of decrease has slowed considerably and has stabilized at about a five percent annual reduction for the past three years. Overall, departments have achieved a 78 percent reduction since the start of the program in June 1972.

- Departments reported 4,487,333 classification actions taken in 1977.[1] While this represents a decrease from 1976, it is consistent with the yearly figures reported since 1972. Of the actions taken in 1977, fewer than 1 percent were classified as Top Secret, 30 percent were Secret and 69 percent were Confidential.

- The 69 percent of the information classified since 1973 assigned the least restrictive classification is attributed, at least in part, to the reduction in the number of authorized classifiers. Most of those involved in the information security program believe that the reduction has had a beneficial effect on the *quality* of classification actions taken since it has forced decisions to a higher level where knowledge of both the program and the intended policy is better understood. One must note, however, that the number of classification *actions* has been relatively stable throughout the period and no correlation has been established between the number of authorized classifiers and the number of classification actions. Rather does it appear – not too illogically – that the number of classification actions taken relates to the number, type, and importance of military, foreign affairs or other events of national significance taking place during the period.

- For the first time the E.O. provided an administrative means for a member of the public to ask for a classified document – the system has worked. Requests have increased from 250 in 1972 to over 5,000 in 1977. Since 1973, in over 80 percent of the cases considered for action, the information has been declassified entirely or in part by departments. Thus departments have tended toward declassification in their processing of these requests.

- Since 1973 departments have received 325 appeals from denials of mandatory review requests; this total constitutes only 2½ percent of the approximately 13,000 mandatory review requests received. Of the appeals considered, approximately 59 percent have been granted in full or in part; and in 41 percent of the cases, the original departmental denial was upheld. This confirms the value of the appeals option and indicates the willingness of departments to overturn prior classification decisons in the interest of public accessibility.

- Further appeals beyond the Department to the ICRC have amounted to less than one-half percent of the 13,077 requests for declassification review. In those cases, the committee has declassified the information entirely in over 23 percent, declassified partially in over 57 percent, and upheld the decision of the departments in 19 percent of the cases.

- A tremendous amount of classified material of historical value has been declassified and made available to the public during this period. To date, the estimate is 215 million pages declassified within the archives alone. The larger agencies, such as DoD, State, and CIA, have their own programs wherein personnel are assigned full time to declassify older agency records.

[1] As noted in our report, this figure is not exhaustive.

Toward the Future

The facts, some of which are stated above, demonstrate that there was progress under EO 11652 and its ICRC monitor. Many problems that have been with the Security Classification System since its inception remain, nonetheless. Improper classification, overclassification, a lack of classification guidance, classification "leaks" and unnecessarily large holdings of classified information are with us today.

If I may capitalize on the *Virginia Slims* ad, we can say that EO 11652 *Came a long way* in increasing the effectiveness and viability of the classification system; *but baby, there's still a long way to go.* The ICRC and the departments which it monitors identified some major "lessons learned" under EO 11652. Dr. Gates has reviewed some of these this morning. Let me name a few others that deal specifically with oversight before I turn to a discussion of the new Information Security Oversight Office.

1. The program review visits conducted by the committee's staff increased security awareness within the departments, assisted in identifying program deficiencies, provided suggested corrective measures and prompted program support from senior officials. However, some of the inherent weaknesses in management by committee have been observable throughout the life of the ICRC. The fact that every item of business had

to be presented to and considered by the full committee was a slow and cumbersome process. This is not a reflection on the integrity or expertise of committee members but is a natural and inescapable outcome of action by committee. Another factor that limited the effectiveness of the ICRC as an oversight body has been a lack of status in an appropriate organizational structure, which caused some departments to take its authority less than seriously.

2. Program reviews conducted by the ICRC staff showed great variance among departments; in the organizational distance between the security staff and top management, and in the relationship of the security staff to the senior official responsible for security. One may say that the higher the security staff in the organizational chain, the more progressive and successful the program. Beyond all doubt, the key to an effective program is *demonstrated support* from top departmental officials. Where lacking, implementation of the order fell short.

3. The requirement for departments to establish and maintain active orientation and training programs for security personnel greatly increased the awareness, interest and support of those working with the system to achieve the goals of the order. Senior officials of most departments recognized that security training is an absolute prerequisite to effective implementation of an information security system, as is true of any system.

4. In general, the statistical reporting system established by the ICRC proved to be an effective mechanism of internal control for the reporting departments. Besides providing needed information to the ICRC, it provided departments with tools to identify problem areas and take remedial action. True also for security managers. However, there *were* problems with some reports. The collection of data for the report of classification actions was difficult and costly for most departments – particularly those creating many classified items (*e.g.,* DoD). A sampling system was authorized for reporting purposes by the ICRC for such cases. *The sample* was exactly that. Classification abuse and unauthorized disclosure reports also produced problems. The committee's definition of these terms was initially overly broad and required revision. Of course there was some natural reluctance of departments to publicize shortcomings. Further, collecting some of the data required was not considered cost effective by some departments, because their systems did not produce requested data. Our base of experience should be helpful in determining the feasibility or cost effectiveness of some reporting requirements.

I think the new Order gives very clear marching orders to the Director of the ISOO. The key word is "openness." Clearly, that is the yardstick against which all actions will be measured. We talk a lot about "openness," but we – many of us – have been brought up in an era where it was policy to err on the side of secrecy. Let us examine what openness means in the context of national security. The United States has always been known for the relative openness with which it conducts its official business. This is entirely consistent with democratic theory, which calls for an informed citizenry able to evaluate the performance of its elected representatives. The new Order will increase openness in government by limiting the use of classification and assuring more rapid declassification of government documents relating to national security. It is the latest in a series of attempts by the Executive Branch to accelerate the availability of government information.

That the public's right to know and the government's duty to protect is a dichotomy has been pointed out and discussed by many. Similarly, other related elements have been presented and discussed many times, points include:

- The concept of an informed citizenry is implicit in the rights guaranteed by the first amendment.
- A "popular" government which fails to provide information about its operations has been condemned by the founding fathers and contemporary officials alike.
- The need for some governmental secrecy was recognized in the constitution itself, and has been accepted by the Legislative and Executive Branches since the early days of the republic.
- The United States plays a dominant role in world affairs, and confidentiality is a prerequisite to most of the dealings the Federal government carries on with other nations. Confidentiality is desirable not only to protect the interests of the United States, but to create an atmosphere conducive to productive and uninhibited negotiations among all parties concerned.

We can sum up by saying absolute openness is as unattainable and unrealistic as absolute security or secrecy. But it is a goal.

The ISOO for the Future

Dr. Gates has covered most of the significant features of the new Order. I plan to concentrate on that provision establishing the ISOO and outlining its responsibilities.

The Order states that "The National Security Council . . . shall provide overall policy direction for the information security program. The Administrator of General Services is responsible for implementing the program through an Information Security Oversight Office, and for appointing a full-time director "subject to approval by the President." Although the ICRC will be abolished, the new Order provides for the establishment of an Advisory Committee comprised of representatives of selected agencies. This will provide a forum wherein security problems common to many agencies may be fully considered within the broad base of experience of the various agencies. Further, recommended courses of action can be developed upon which the Director of the Oversight Office may act.

As contrasted with the ICRC, the scope of functions and responsibilities assigned to the oversight office have been expanded considerably. Some highlights are indicative:

1. The Order tasks the oversight office to ensure compliance. To this end the office is authorized to conduct on-site reviews of agency programs as well as to require reports. This includes all agencies handling classified information. The specific mention of on-site reviews in the Order is new, and we hope this fact will give the "reviews" more clout.

2. The archivist of the U.S. acts on requests for declassification of presidential material over 10 years old. If he denies a request the requestor may appeal to the oversight office. This is very similar to our present appeals system.

3. Agencies must publish implementing directives as well as guidelines for declassification. These must be reviewed by the Oversight Office to insure conformance with the Order and the implementing directive. The Oversight Office has authority to direct changes if necessary.

4. A significant new task for the Oversight Office is the development and promulgation of directives for implementation of the Order. This could have far reaching effects with respect to standardizing procedure.

5. The Director of the Oversight Office will have authority to classify and declassify information in any agency not only upon request but in connection with on-site reviews and inquiries.

6. As did the ICRC, the Oversight Office will consider and take action on complaints and suggestions from persons within or outside the government with respect to administration of the Information Security Program, and

7. As did the ICRC, it will report annually to the President as to the status of implementation.

It is my view that if the oversight body is to achieve some measure of success in advancing the goals of the Order, it must provide strong leadership and be actively involved. It must go further than accomplishing the specific tasks outlined in the Order. For example, in order to foster a viable Information Security Program, I believe the Oversight Office should:

- Extend on-site program review coverage to contractors and to activities outside the Washington Metropolitan area.
- Expand on-site program review visits to include in-depth coverage of physical security and personnel security programs.
- Assist agencies in establishing ADP systems to obtain more precise data for information security management.
- Develop information security education briefings and training aids for use throughout the Executive Branch.
- Sponsor, assisted by the Defense Industrial Security Institute (DISI), information security training sessions for use by all agencies in the Washington Metropolitan area.
- Establish a repository of security education material for use by agencies in the Washington Metropolitan area.
- Work toward the establishment of a civil service career field for information security management.
- Develop basic security forms for standard use throughout the Executive Branch.

- Develop and promulgate basic information security procedural manuals for use throughout the Executive Branch.

Now, accomplishing all these things is going to take resources. The existing staff of the ICRC will prove a most valuable asset in ensuring a smooth transition, continuity and in providing the necessary "know-how" to oversee the program. The rapport and the mutual sense of cooperation that have developed between the ICRC staff and the agencies' security staffs will also help to make the changes introduced by the new Order less disruptive. However, in spite of the motivation and expertise of the ICRC staff, the fact remains that an expanded oversight role demands an expanded staff. My estimate is that oversight under the new Order will involve at least 30,000 man-hours per year, which equates to a staff of 14 persons. This is considerably larger than our present staff of 8, and considering the present era of austerity there is a question about whether 14 will be authorized. But nevertheless, that's what is needed.

In Conclusion

All of us fully realize that the program goals prescribed by the Order will not be self-fulfilling. We all know that goals are only achieved with effort and after completion of specific tasks. In the months ahead, the ISOO will be defining the tasks that must be accomplished to achieve the goals of the Order and will be monitoring departmental programs to oversee full implementation.

The mechanisms that the ISOO will use to monitor and evaluate agency compliance with the Order and implementing directive should not differ significantly in *nature* from those used under E.O. 11652. There will be significant differences, however, in *substance* and *emphasis.* Departments will continue to be required to submit statistical reports. However, these will be simplified and streamlined to reduce paper management costs and to provide more meaningful implementation indicators. In anticipation of this need, the ICRC staff has begun a study aimed at developing simplified forms and at identifying meaningful reportable data. The ISOO will continue detailed on-site reviews or inspections of departmental implementation, but they will be in greater depth. Some may be unannounced. These reviews have proved to be the most effective means of ensuring implementation. Through such visits the office staff will learn of implementation problems faced by agencies and will be able to identify areas where greater oversight is needed or change is required.

We must all remember that the ultimate success of any program depends upon the motivation and dedication of the individuals that work with it. Your help and that of your security staffs is needed to make the system work. *GET INVOLVED.* Contribute your resources of experience and knowledge to the achievement of a more viable program.

Finally, let me state that establishing reforms in the area of classification and declassification is a slow and painstaking process. As we all come to appreciate the need to establish and maintain a stable, deliberate and responsive program the results will be increased openness and better protection of that material that truly requires it. Any retreat from the spirit of disclosure and access embodied in the new Order would only serve to further erode confidence in government when we need it most.

Questions and Answers

Question: During your reviews, did you find a need for different rules for different kinds of material? For example, presidential versus operational type papers?

Answer: Yes, there is a definite difference between the two. As you know the only request route for a presidential paper is provided by the Executive Order, not the Freedom of Information Act. But, there is a problem with presidential papers. When a President leaves office, the papers are assembled and sent to a holding area or to some library. Many times agency records are included as well. An agency record is required to be under the Freedom of Information Act but if it's in a Presidential Library, so you can come in only under the Executive Order. So, there is that problem.

I believe the changes in the new Order will resolve that problem. If the Archivist determines that a paper that is in such a library is an agency record, he will forward that record to the agency for direct response to the requestor.

Question: An inaudible question was raised relating to personnel clearances.

Answer: A sizeable number of smaller executive departments or agencies do not have the trained security people that a department such as DoD has. Therefore, there is no program of substance established. We want to try to encourage people to think about their real requirements for clearances. I'll give you a good example of the need.

We went to Civil Aeronautics Board where almost everybody in the agency had a security clearance. We talked to management and found that they could get rid of 60 percent of their personnel security clearances. That is a substantial saving in money and the associated investigative resources. It's not that either the ICRC or the new ISOO is to be pursuing personnel security *per se.*

There is a different field that comes to mind, however – records management. There needs to be a much closer tie between declassification and records management. Let's get rid of the mountain before one must review.

Question: You suggested educating in the Washington Metropolitan Area with the help of DISI. Are you trying to train on a national level so that those trained can branch out "and teach people in the field that work in both industry and government?" A matter I was discussing earlier.

Answer: I think that's a very good question. We have departments and agencies that are not staffed with people who have been involved with classified information. We want to give them at least some working knowledge, and, yes, I think that once they are trained, they can return to their agencies and improve the awareness and understanding of others.

DLA – ADVISOR OR ENFORCER

Colonel Jack G. Pruett, USA
Executive Director, Industrial Security, Defense Logistics Agency

As many of you may be aware, the April issue of *Security Management,* published by the American Society for Industrial Security, contained a number of articles concerning the industrial security functions of the Defense Logistics Agency. On its cover there appeared boldly the question, *DLA – Advisor or Enforcer?*

Apparently the caption caught the eye of your Program Chairman who asked that I elaborate on that subject. A rephrasing of the question might clarify it somewhat. Is the mission of the industrial security element of the Defense Logistics Agency one of advice and assistance or is it one of enforcement of requirements? I'm happy to be able to address the question before a forum of this type. All of us are part of the security community. Each of us must periodically explain where and how we fit in the management picture of our organization. Are we advisors – or are we enforcers? I intend to give you the benefit of my own conclusions and show you why I think we are both. If you have read those articles, you may have drawn your own conclusions already. Before someone gets the impression that enforcement has become the theme in DLA – just because I come from a Military Police background – I hasten to point out the sequence in which the terms are used. Advice first, enforcement second!

Perhaps it would be wise to note that enforcement in the context of our various functions does not mean *compel* in the sense of inflicting punishment, imprisonment, or death as some popular fiction stories would have us believe the term "Enforcer" implies.

Each of us practices enforcement in our personal lives. It may be control of household expenses, or setting deadlines for the youngsters on study times, or perhaps ensuring that chores at home are accomplished. Normally, the mere statement of the requirement of guideline is all that's needed. With proper motivation it's rare that more drastic measures are needed. And so it is with our missions in the industrial security field.

Let's look for a moment at the four primary areas we wrote about in the *"Security Management"* articles. First, I'll mention the job we're called on to do in the Safeguarding of contract related Conventional Arms, Ammunition and Explosives in the possession – or under the control – of DoD prime and subcontractors. We survey these contractors to ensure that these items are adequately protected to preclude theft, misappropriation or loss. Where deficiencies are noted the Industrial Security Representative makes appropriate recommendations. Unless the contractor is required by contract to meet specific standards, our recommendations constitute advice only. Compliance by the contractor is then voluntary. On the other hand, if standards are established in the contract and deficiencies are detected, the contracting officer can invoke certain sanctions for failure to correct the deficiencies. You'll note that we in security make recommendations and supply advice, the enforcement is up to others.

A second area encompasses the periodic surveys our people conduct of critical industrial plants, known as

"key facilities". Here we are totally in the advisor role. There is no enforcement in any formal sense of the word. There is an external factor which could be labeled enforcement, of course. That is the pressure on management to stay in business, to be able to meet emergency conditions and to be able to provide their service or product when called on to do so. Certainly DLA is not the enforcer here.

The Defense Industrial Security Program is the third area where both advisor and enforcer roles are thrust on us. In this program we attempt to assure the safeguarding of classified information entrusted to American industry by the United States and foreign governments. The whole process starts when some government or industry element says they need the services of some contractor, and those services will involve access to classified information. Our first contact with a facility is completely advisory. We inform the contractor of what is required to be cleared, what is needed to maintain the clearance, and what the requirements are for safeguarding classified information or material. After clearances are granted, we inspect periodically to evaluate how well the contractor understands and implements the numerous safeguards and procedures required. Each of these inspections transcends the advisory relationships between contractor and cognizant security office, and between the Industrial Security Representative and the people he or she contacts. Three things are happening:

- We check to see whether security measures in effect are adequate
- We counsel those with whom we come into contact on either what's needed or confirm that existing practice is adequate.
- We identify deficiencies

It's obviously the third item which gives rise to the concept of enforcement. If and when deficiencies are discovered, counseling is ignored, and deficiencies remain uncorrected, *then* we move into the enforcement concept. In such a case, we advise the contractor's customers that major deficiencies exist and prohibit additional classified information from being furnished. A more severe case could result in revocation of a facility's security clearance. These are *enforcement* measures that we can take. On the other hand, there are different actions that can be interpreted as enforcement – prosecutions where violations of law occur, placement on the debarred bidders list, and other more subtle forms of persuasion.

How often does the enforcement role come to the fore? Once or twice a year? Daily? My best answer to this would be that it depends on what you wish to label an enforcement. For example, there were two facility inspections resulting in unsatisfactory ratings during fiscal year 1977. Hardly impressive to those who are punitive-minded or equate success to number of "punishments" meted out. Now the figures become a little more impressive. During that same period we sent letters to management on 257 inspections where major deficiencies were detected. These letters left no doubt that we expected the deficiencies would be corrected and we scheduled follow-up inspections. Additionally, minor deficiency letters were sent to management on 5,129 inspections. Finally, 3,562 inspections had deficiencies corrected on the spot. There you have the facts and figures. There is one thing though that might swing the balance towards the "advisor" side of the scale – certainly so as far as DLA is concerned.

If one were to presume that our major thrust was towards enforcement, one would not expect our continued level of efforts in the education and training fields. Mr. Robert Green will elaborate on a specific high priority effort – the Defense Industrial Security Institute. One of the articles, that I mentioned generated my topic, gave a brief insight into our efforts. This year we are trying to revitalize the Education and Training efforts in the nine regions, and at the same time invigorate the role of our regional Classification Management Specialist. In my view, these actions are a stronger endorsement of my thesis than is the opinion of a few who would have you believe that we're oriented primarily toward enforcement.

My final thought on the question of whether we are *Advisors or Enforcers* rests on the functional difference between *security* and *law enforcement*. Both have the same objective

- Prevent violations
- Investigate a violation, if one occurs, and
- Identify or apprehend the violator.

I maintain that the difference lies in the choice for emphasis among these three objectives. We in security place the major emphasis on prevention *before* the fact of a violation. The emphasis in law enforcement, because of limited resources, is investigation and apprehension *after* the offense has occurred.

As long as I can influence the direction of our efforts, we'll continue to place our emphasis on advice and assistance – using our powers of enforcement only as the last resort.

Questions and Answers

Question: Colonel, considering what you might be able to predict of the future for the classification management specialist, will they increase their role, decrease their role, or remain essentially as they are?

Answer: That's a good question. I have a very concerted effort to completely staff the DCASR's throughout the country with dedicated CM specialists not responsible for other aspects of the industrial security program. Not only in the classifcation management arena, but also in the education and training arena and they are very definite formal programs. Some may not be aware of some of the things we're doing in the Education and Training area; particularly in taking road shows to the field. Several of you were in California when we ran our first Industrial Facilities Protection Program, "road show" in Los Angeles . These are planned for the various DCASR areas throughout the United States for the next eighteen months to two years. The "road show" takes staff from Washington and elsewhere to whichever area to present a course. We are increasing the number of such courses. Our greatest participation, for example, is in the *information* arena, as might not surprise you of NCMS. We are hoping to be able to train more people still. I personally have strong feelings about education, including my own staff. I get them out. They are not only on the road constantly but also I keep sending them too to schools to enhance their education.

Going back to the basic question on classification management; I believe you will find, in less than the next 12 months, that we'll have a strong revitalized, if you will, program in the field. In my view it has been neglected. I think the neglect is in terms of priorities as they're placed upon us – resource limitations, if you will. We're getting greater visibility, more interest in our programs, and I must say that the Director of DLA, General Vaughan, and his staff have given us strong support over the last six months to a year to really push our program. We're moving, we'll get there.

Question: Voice (inaudible).

Answer: Yes, in excess of 25,000. I started to mention earlier that there was a tremendous workload. I do analyses and comparisons constantly, based on prior years but there are some gray areas that relate to certain types of contracts, "black," if you will. However, the total in round figures runs approximately 25,000 per year. When you then take only two unsatisfactory ratings from a group of such size, it's a relatively inconsequential number and I think that our people are doing a job. I believe the effort is mutually supporting.

IMPACT OF THE NEW EXECUTIVE ORDER ON USER AGENCIES

Arthur F. Van Cook
Director for Information Security
Department of Defense

As Mr. Cooke noted in his presentation, many provisions in the new Order have been in operation in the Department of Defense. Consequently, we believe that the Department of Defense will have little difficulty in adapting to the new Order. Some agencies, as Mr. Wilson from the Central Intelligence Agency likely will cover, may have more work to do. I will cover some of the known changes such as marking and our view of changes in emphasis on, say, our educational and training efforts.

I plan to cover the highlights of the Order as we know it now and then address each as I think it might affect the Department. Keep in mind, Mr. Cooke commented, the Order is just a skeleton; one hopes that the language will achieve the President's objectives as set forth in Presidential Review Memorandum No. 29. Then also that the "gray" areas in the order will be clarified when the implementing directive is issued.

In connection with the directive, Mr. Wells didn't emphasize that during its interim period before the Order comes into force on 1 December, functions required to be performed by the planned Director of the Information Security Oversight Office will be performed, as the draft Order establishes, by the Interagency Classifications Review Committee (ICRC). So, actions such as

- Issue of an implementing directive, with the concurrence of the National Security Council, and,
- Review of agency implementing regulations

will be a responsibility of the existing ICRC of which Mr. Wells is the Executive Director.

As I mentioned, we expect the directive will clarify and expand on some of the provisions of the Order.

We expect further, that the DoD regulation will, in turn, contain specifics on how the DoD will make fully effective both the Order and its implementing directive. Mr. Cooke has mentioned that we have already started on our directive. We hope to have a draft for circulation and comment shortly after determination on the provisions of the "NSC" directive.

All of the implementing directives/regulations will be aimed toward achieving the Presidential goals as set forth by Dr. Gates as contained in Presidential Review Memorandum No. 29 of 1 June 1977.

As Mr. Cooke and I have mentioned, our program reviews in the Department of Defense – from the time the Order is signed and until it becomes effective – will be aimed toward education. People from my office will visit industrial facilities and major commands of the Department of Defense solely with a view to educating. That is to explain perhaps what the provisions of the order are, what the provisions of the regulation will be, what impact those regulations will have on facilities visited and will solicit comments from those activities, so that we can put out a policy that is reasonable. These will be our objectives and so our initial reviews during the time between signing the Order and its effective date will be aimed along these lines with those objectives. Now let's take a look at the Order itself and discuss how its provisions might affect specifically the Department of Defense and defense industries.

Classification Authority

With respect to classification authority, the change is almost imperceptible. We will still designate the authority in the Department of Defense as we have in the past, and we'll give that authority only to those who have a need to exercise it.

However, in connection with delegated authority, there may be a change. In parts of the Executive Branch there may be an increase in the number of top secret classification authorities – I'm not certain of this. The reason this may be is a provision in the Order requiring that security classification guides be approved by a top secret classification authority. Previously in DoD, for example, if we were to develop a security classification guide in which there was no exempted information category and which dealt only with information at the secret or confidential level in either the General Declassification Schedule (GDS) or Advanced Declassification Schedule (ADS) it could be approved by a person with the appropriate level of delegated original classification authority (*i.e.*, Secret or Confidential).

Under the new provisions, however, *all* security classification guides – irrespective of classification level or duration of classification – must be approved at the top secret authority level. Now, whether this will have an effect across the board in the Executive Branch by requiring designation of more top secret authorities for that purpose, I really can't tell you at this point. We hope it will not. In the Department of Defense we have something on the order of 477 top secret classification authorities. It may be manageable merely to require an original top secret authority to approve all guides in his area of jurisdiction; we'll have to see. Other than that facet, there is little change for DoD in the requirements of the new Order affecting delegation of classification authority.

Classification Requirements

Turning to the area of classification requirements. The new Order establishes that classification is a two step process and establishes classification criteria. Within the Department of Defense that's been our policy and procedure for some time. In fact, we have classification criteria. It's not enough that information may fall within the classification criteria; but there must also be a specific degree of damage that can be related to the effects of an improper release of information or material.

The language of the new Order requires a showing of *identifiable* damage. Because of an established practice, there will be little perceivable change in this area.

An element of change is the limitation on duration of classification. There is a conceptual change from the automatic downgrading and declassification system as we have come to know it. In what now must be considered historical perspective, going back to about 1967, I wrote an article in the National Classification Management Journal which dealt with downgrading and declassification – a subject which we'll be addressing tomorrow.

In that article I was critical of the long period of time that it took for things to go from initial classification to declassification. It was a 12 year time span between changes in those days. I was an advocate of substituting for that system a more accelerated

automatic downgrading and declassification process, and it only took about 5 years to sell that proposal first in the Department and then to the Executive Branch. The concept is reflected in Executive Order 11652. Over the years I have been a staunch supporter of an automatic downgrading and declassification system. But reflecting now, there were, perhaps, unperceived faults. Consider the concept; the time-length for classification was dependent on the level of classification or the level of sensitivity of something as it *entered* the system. If it went in as top secret, under the existing EO 11652, it would stay classified for 10 years. Why? Because the level of sensitivity as it went into the system was at top secret. If it went in as secret, the duration of classification was 8 years; at confidential only 6 years.

The duration of classification should not be solely dependent on the level of sensitivity of something *at the time of its preparation*. For example, something that is top secret today could very well be unclassified in two weeks – after the occurrence of an event. On the other hand, something which is confidential today may maintain that level of sensitivity for 20 years or longer. So, the *duration* of classification should be dependent on the loss of sensitivity with the passage of time, not its initial classification. The draft of the new Executive Order eliminates that concept. Further, its requirements for citation of an extension authority at the top secret level reduce the potential for unthoughtfully extended classification.

Another comparison of DoD practices with the expected changes established in the forthcoming Order can be found by examining further the means by which classification can be extended. In current DoD regulations only a GDS or ADS decision can be made by a person with original Secret or Confidential classification authority; anything requiring further protection must be a decision of an originial Top Secret authority. This is in accord, of course, with the concepts of EO 11652 and its implementing directive. That, then, is not dissimilar to the planned six-year limit. Extensions beyond six years, recalling my previous comments, will require the top secret authority (or the head of an agency). A difference noted previously is that *20* years is the maximum for extension rather than 30. Then, as before, only heads of agencies may decide *personally,* that further protection is required.

These two concepts are newly contrived and there will be a learning process; we will have to get to the classifiers and help them understand what authority they have, and how they may exercise it. Again, the impact is educational. We will need resources. We're going to need people in the education process to get around and get the word out. That's been a problem in the past, it is in the present and will be in the future.

Identification and Marking.

There are some new requirements in the marking process. Classified documents now must show an identification of the classifier and also, when applicable, the identification of the authority extending classification beyond a six-year period, as well as the justification for such an extension. The Order provides that that justification may be a citation of criteria which is included in an agencies' implementing regulations.

There is a potential problem here both for agencies and the industrial community. For example, a citation on a DoD document arriving at the State Department that the reason for the extension was criterion number four would be meaningless; similar perhaps to a "Classified by 00784" in our current system. What industry would do in addition to citing their DD Form 254 is unclear. It is an area where clarification is needed in the NSC approved ICRC implementing directive. A related facet of this problem can be found when considering what to do about electrically transmitted messages. Some solution for how this information will be shown – to comply with the requirement – will have to be developed, or it could be a costly requirement.

Another marking potential found in the order permits an originator to affix special dissemination or reproduction limitations. While new to the Order, DoD has had some brush with like requirements before.

Prohibitions.

New in the Order are prohibitions against classification under stated circumstances. DoD has had similar prohibitions against classification, and I believe enforcing those prohibitions will not pose a problem.

Derivative Classifications.

Turning to another new section, there is, for the first time in an Executive Order a section on derivative classification setting forth the requirements. As I just mentioned, I believe we need clarifying language in the ICRC directive to establish what marking is required for a derivatively classified or marked document. How guides and DD Forms 254 would reflect extensions

and justifications is a potential problem that needs to be solved.

Declassification and Downgrading.

A provision in the Order encourages the delegation of declassification authority to the lowest practical echelon. This is not new but the language is more explicit and more forceful. I believe the effect will be to facilitate the declassification process when industry, for example, is trying to find an authority to declassify certain information or material. We will try to place declassification at the lowest functional level. I personally have tried to do that for sometime under the existing Order without much success. The language of the new Order, I believe, will permit us to get this job done. As a practical example, the Secretary of the Army could give an individual, at a low organizational level, declassification authority over information in a particular functional area. That person need not have classification authority. It appears to me that this will be an advantage for the program in DoD. The policy stated in the Order is that declassification shall be given comparable emphasis to classification. Further, as mentioned this morning, there is the introduction of a "balancing test" in the declassification process – I won't dwell on that.

Systematic Review.

The provisions of the new Order have an impact on government agencies. I might comment that when this Order was being drafted – in its very early stages – people at the National Security Council level, White House staff level, were made aware that moving to a 20-year declassification concept, versus 30-years, was not "free." In the Department of Defense we estimated a cost of about a million and a half a year with some 80 people needed. As I say, that was made known "up front" very early in the game. If the resources and money to pay for them are not available, the job can not be done. It's as simple as that. With that in mind, the Order will, in fact have a 20 year rule. We have to hope that resources will be made available to get the job done. It's true that there is a 10 year phase-in authorized to get to the 20 year review stage. However resources are needed and one hopes that one will not face the "Take it out of your hide," syndrome. If we have to take it out of our hide, we must recognize that there will be much more "seek" than "hide" and the job is just not going to be done.

Guidelines.

Mr. Cook referred to guidelines that may be applied to 20 year old material. In my opinion, there is not a general understanding of the difference between *guidelines* and *guidance*. Guidelines do not establish that certain categories of identified information are certified by the head of the Department, say, to require classification out to 20 years and may not be automatically declassified but must be reviewed at the 20 year mark. Now, that *is* guidance for *extending* classification of new material, but what also must be done is to prepare guidelines for the *declassification* of 20 year old material, which may be applied to material as it gets to 20 years. That guidance, it appears to me, should be the antithesis of the classification guidelines, used for declassification.

The kind of a concept we're working on in the Department is a single set of guidelines. I think it's not enough, as the Order now prescribes, that these guidelines shall identify specific categories of information which are going to require review at 20 years. That's not complete. That's a guideline to extend classification, but we have to build into that guidelines for declassification as well which will be applied when we hit that 20 year mark. We hope the point will be clarified in the ICRC directive.

Foreign government information.

As you may not know this category will be exempted from the 20 year automatic declassification or review provisions of the Order. That information will not need to be reviewed until it reaches its 30 year mark and then may only be declassified in accordance with guidelines jointly development with the government concerned.

Mandatory review for declassification.

In the new Order there is no timeframe or limitation, with the exception of Presidential material which Mr. Wells addressed. However, as you know, people can now ask for review under the Freedom of Information Act of information only 10 minutes old. We don't anticipate any great change to be caused by the provisions of the new Order. The language was intended to conform with the FOIA.

Downgrading.

The Order only provides that if downgrading is appropraite, do it. There's no automatic downgrading provision in the Order. We'll be talking about downgrading tomorrow but there's no real value to downgrading,* although there are certain exceptions.

Special access programs.

These may be created or continued only by agency heads. After a five-year timeframe they'll automatically terminate unless they meet certain criteria prescribed in the Order. This, I think, is helpful to us in the Department of Defense. We've got an awful lot of compartmented information and the compartments should be reviewed. There are special access programs that have been in being for years and probably there is no current requirement to continue some or many of them. So, it is desirable to examine these things and see whether they meet the criteria of the order; if they don't discontinue them. There are some exceptions to the automatic five-year termination procedures specified in the Order. Those exceptions cover programs involving foreign governments and international organizations.

Access by historical researchers. These categories including access by former presidential appointees appears to have no substantial change. There is a provision in the order which puts some controls on reproduction, however, I see no important change. A difference to be noted is that this is now in the Order rather than in the directive as it was before.

The Information Security Oversight Office. This has been covered by Mr. Wells and I will touch on only a couple of points that will cause some change for DoD. There are *Many* responsibilities given to the Information Security Oversight Office and it has to be adequately staffed.

An impact on expanding that staff, of course, will be that we'll have more program reviews and more visits. From the point of view of DoD, we don't believe we need a whole lot more, but we welcome those because good things come of it, and they are all designed to improve the program and we're all for that. The Information Security Committee was mentioned by Bob and, of course, that Committee now as contrasted with the ICRC, is in an advisory role.

Responsibilities of Agency Heads. I think you're most interested in these. A most important one from your point of view is that the Order makes it mandatory that agency heads assure the issuance of security classification guides.

DoD and DoE have been in the business of working with guides. On the other hand, agencies like CIA, State and others, have not been. In my opinion, the most difficult kind of guidance to develop is in the areas of intelligence, foreign relations, and operations. Scientific and technical we can pretty well get a handle on and develop security classification guides in those areas that are meaningful. In the intelligence field, foreign relations, and the operations end of the business, they're more difficult. I know there's going to be a great impact on other departments in the Executive Branch with respect to getting out and promulgating security classification guides.

Under the new Order as in the old, the department heads are required to designate a senior official who will be responsible for program implementation in the department and also a senior official to chair a departmental committee which will be formed to listen to suggestions and complaints concerning implementation of the order. So, there is essentially no difference.

Agency heads are required to have a security education program and this, as I mention is going to be our biggest effort after the Order is signed. As those of you who were around when the other executive order were issued, that was our biggest job was to get the people educated as to what the new ballgame was all about.

Safeguarding practices are required to be reviewed and those which are duplicative and cost ineffective are to be eliminated. I hope that in reviewing these things we do in fact eliminate certain double standards that we have between defense and industry and I think we'll be working on that and giving that a lot of attention in the days and weeks ahead.

So, in summary, those are the provisions of the Order. I believe it will be an education process. I think that the education is going to focus on the new concept of classification guidance – new outside the Department of Defense – and on downgrading and declassification to bring about more openness in government.

---

*Ed. Note: It happens that shipping and mailing costs for either material or documentations, respectively, *are* valuable.

Questions and Answers

Question: Will we have to examine and remark current material?

Answer: There will be nothing in the forthcoming Order regarding retroactive provisions. What I mean by that is there's nothing in this Order, and there should not be in the implementing directive, which will bring about a review of current files to change downgrading or declassification determinations. That never works. It just does not work and we might as well recognize that up front. So, we take it from this day forward and if something is already marked for automatic downgrading and declassification, let it run its course. Let it go, but don't try to reach back and resurrect documents for review for earlier downgrading and declassification. It just won't come about but there's nothing in this order that will make us do that and there will not be anything to my knowledge, in the implementing directives that will bring that about. I just think that's wasteful.

Question: With reference to your answer, is it not possible that implementing instructions would result in the generation of new classification guides with differences in downgrading or declassification actions which would affect documents in storage?

Answer: I think the new provisions of the Order will certainly force a review of security classification guides and bring them into line with the changes, but from the effective date of the guide forward. Not to require people to retroactively apply those classification determinations to something that's already done.

Question: Let's assume that I have a document here that is scheduled under the present declassification schedule for declassification in 1980. The new Executive Order and implementing instructions result in the publication of a classification guide which will declassify this same information in 1979 instead of 1980. Is it not then permissive for me to remark this?

Answer: Permissive, yes, and I think that our provisions in the Department of Defense would be that if that document is removed from a file for use, that would be the time to do it. What I'm getting at is that we shouldn't have anything in our implementing directives that will *force* a review of all previous documentation for purposes of taking that kind of an action. If a document is removed from a file for whatever use is going to be made of it, that's the time that you should take a look at it and apply the current guidelines or guidance.

Question: Will Restricted Data and Formerly Restricted Data still be exempt from automatic downgrading?

Answer: Yes. There's nothing in this order that will interfere with or be contrary to the provisions of the Atomic Energy Act of 1954.

Gene Wilson
Information and Privacy Coordinator

Some of you may remember that two years ago when I talked to this group, the business at hand was freedom of information, the agency's difficulty in releasing information, and the bitter pill that it was. Well, since that time we've averaged 65 to 70 requests a week – every week – going out to the public. Most of that material had been previously classified material. There has been so much material that has been released to the public that my agency now refers to me as the guy who sells yesterday's secrets for ten cents a page. I find that when I get on elevators in my building everybody else gets off.

I haven't really been part of the group in Washington that's been putting the new Executive Order together, so I thought I would take the approach as to how I as a manager in an agency with a high percentage of very sensitive and classified material will react to the new Executive Order. Therefore, I felt it was timely to go into the draft in great detail with the people from CIA who have been working on it. I decided to take the approach of color coding the new Executive Order. I identified some things as green and green is go. It's good. Some things are red, which means a problem, and some things are gray, which means it will take months probably for us to really decide about. Let me start out with the color coding.

GREEN – In going over the Executive Order it appears that those sensitive things within the CIA that must remain sensitive will be able to be protected. Primarily of concern to us is our protection of intelligence sources and methods. We've been able to protect those throughout the FOIA battles and it appears that the new Executive Order will continue to permit us to protect all of our necessary sources and methods. An intelligence agency without intelligence sources is not an intelligence agency.

RED – Declassification review after 20 years; the red aspect here is volume. If the classified documents that we hold within our agency – from 1947 when we were a new agency until 1951 – were stacked next to the Washington Monument and equal in height, it would result in seven stacks. Now, that means someone is going to have to go through document by document, in some cases page by page, to make sure the information is not provided by a foreign government and requires protection for a period of time. So it's a tremendous review process. It's a review process that has now been started. We have thirty people engaged in it full time. In a few more months we'll have forty people working full time going through these documents. These are not and cannot be brand new people. They must be experienced agency people who can identify the true sources and methods that we have to protect.

GREEN – It appears that the new Executive Order will permit those lower level employees within the agency who write classified documents everyday, to have classification authority and continue writing those documents in a classified manner.

GRAY – Who really is going to be responsible for implementing this new Executive Order? The Office of Management and Budget wasn't too exicted about it. Possibly it will go to the General Services Administration, but is there expertise in GSA to manage something like this or will the management of this fall back into the process of appeal? Will the National Security Council be the one that takes up the ultimate management? It's a gray area for me. I'm going to have to find out as we go in time.

GREEN – This basically is an area where I think the agency has a lesson to learn from the Department of Defense. Derivative guidelines, derivative classification. I find two aspects in derivative classification. One aspect is traditional derivative classification where an analyst is reviewing material, he's rewriting material, he's editing material that's coming from a sensitive source. That document that he's using is a base of his information already classified. He will be able to use the classification from those source documents to carry on into the document that he's creating. He needs that.

The other aspect of derivative classification is that of guidelines in which a top secret classifying authority will provide guidelines to other agency employees that will guide them and give them the authority to retain the classification on those things that have to remain classified.

GRAY – Declassification after 20 years on an item by item basis. I go back to an earlier concern. Although we have those seven stacks of documents sitting next to the Washington Monument, once we get into the early 1950's we find that the volume of records within CIA tripled for the next few years. It's a volume that's almost incomprehensible in terms of going through on an item by item basis, particularly when you know that many of those documents are documents that you will still not be able to declassify after 20 years.

If you recruit an agent at the age of 20, he may still be working for you at the age of 40. That is no time to declassify a document and *burn* him someplace. This has already imposed an incredible burden (and expense). A good example of the burden I cited earlier; we now are using 110 people in the agency to handle FOIA requests. Soon we will be using 40 people for 20 and 30 year declassification. That's 150 people. We do not have even one individual in the agency who's a full time classifying officer. So at times, I feel that perhaps the cart's ahead of the horse.

GREEN – The requirement for a mandatory review within a period of time is, I think, essential. I believe it's good "open government" to be able to establish some period – some reasonable period – of time in which one must review documents. Otherwise, there's a tendency for the bureaucracy to automatically stamp a document that will keep it classified for an indefinite period of time and I don't think that should happen; *even* in an intelligence agency.

Another point that may help is that providing guidelines may well provide a *Green* since guidelines even within a small agency like the CIA, will generate considerable activity in reviewing what the classification process *is*. And, the people on the operational side probably are going to have to write a set of guidelines and the people on the production side (the analysis side of the intelligence business) are going to have to have guidelines. There is an automatic training process involved here because in order to establish guidelines and to have guidelines properly approved, means that where there is very little attention *now* on classification problems, there will be considerable attention, and I think this is good. It's positive.

As a personal recollection I, as a classifying officer for 10 years, remember that the extent of my classification knowledge was how many rubber stamps my secretary had; and I think knowledge needs to be expanded rapidly, and the new Executive Order will in a sense force that – that conscious decision – deciding

whether that document is classified or is it not classified? If it's classified, *why* is it classified?

GREEN – The identification within the Executive Order, the documents originating from a foreign government will retain that classification. This has been a continuous problem with us. In terms of our relationships with a number of foreign governments, we have a large list of complaints from other foreign governments over the inability of the United States to maintain their secrets. Serious concern raised, particularly in the intelligence field. We're finding this more and more being raised in the business of freedom of information requests – where you're releasing information that you *thought* you had gone through and you *thought* that you had removed all the details which would pinpoint who the source was or is.

Confidential classification in the new executive order will now require identifiable damage. I think this is a execellent process. This is a good green light.

All appearances from examining the drafts of the Order suggest that the *number* of classified documents will not change much. At least as it relates to our agency, I do not find any portent of dramatic changes in the number of classified documents.

The change in the number of classified documents as far as we were concerned *was* dramatic after EO11652. Prior to that time, there was a tendency to classify automatically. EO11652 did make significant progress in forcing individuals who do work with secrets everyday to consciously think again about a given document. It is classified or is it not classified; if so, show why it's classified. This should continue under the new EO.

RED – It's almost impossible for a CIA classifier to identify a date of automatic declassification. Much of the classification within an intelligence agency depends on the source and that source may require continuation of a protection for a long period of time. Even though the agent no longer works for you, you have an obligation to protect him as a source for an indefinite period of time; because, if you do not protect your sources and agents today, you will find it difficult to recruit them tomorrow. Remember that the human source in intelligence is a vital part of intelligence community.

GREEN – Mandatory paragraph marking. I put a green light on that. Even though the earlier Executive Order requested it, I found that CIA kind of ignored this; we just started doing paragraph marking about six months ago. This change is difficult; principally because when one has been thinking about classification on a whole document basis, one has tended to ignore and not consider a given paragraph. However, when you're in the FOIA business, you *like* classification markings. Besides, I think marking is mandatory and it reflects *desirable progress in a needed area.*

GREEN – The balancing test. Believe me, from the Freedom of Information Act I have learned the balancing test the hard way. A good example, to give insight, occurred last Thursday. I spent all of that day preparing for a 10 o'clock Friday morning court; to defend the fact that we cannot give out information regarding a Russian defector. After spending all afternoon preparing to testify and say, "Sir, I can't answer that," the judge threw out the case by 5 o'clock on Thursday. Sometimes it gets close.

The balancing test is good. FOIA provides to some extent a balancing test on the judicial side. This is good. Admittedly there are some judges who may not be the most expert in making such a decision, but the process is good. The process says an agency who wants to defend whether a document is classified has to conscientiously prepare an affadavit, go into court, showing why that document must be classified, and why it must be protected. I have found that when one signs an average of two or three affadavits or interrogatories in a week, one does a thorough and serious balancing test; it is a worthwhile procedure.

A problem in context of FOIA that concerns me is the backlog. When I left Washington, we had a backlog of 2,900 unanswered requests and a law on the books that says you will answer within 10 days. That's about a year's backlog. In the appeal process, through which you go in judging documents, we have a backlog of about 300 appeals – that's about 2-1/2 years backlog with our present staff of employees, reviewers, and lawyers. We have been invited into court on about 115 cases. Of the 30 cases that have been resolved we have won. We have been able to defend the fact in court that the documents do need to remain classified and that are identified as classified. Also the courts have uniformly upheld the need to protect intelligence sources and methods.

GREEN – The fact that the Executive Order recognizes that there are times in the life of a government agency when you can neither confirm nor deny the existence of records is good. I have found that this is a valuable tool, a valuable tool in the intelligence FOIA process.

When someone comes in and asks, "Is Sam Jones an agent for the CIA?" I can write back and say, "We will neither confirm or deny." This would protect Sam Jones if he were an agent. The difficulty with something like that is that I quite frequently will get letters from Suzie Smith in Lower Podunk who says, "The man across the street looks kind of strange and therefore I have come to the conclusion that he must be a CIA man." If I write back to Suzie and say, "I can neither confirm nor deny," I've set the man up as you can imagine.

But such a capability and authority is necessary. We have requests from such as the *New York Times* on whoever may have been associated with them and us. And from various colleges regarding faculty-CIA associations or student-CIA associations, as well as many others. We need to be able to maintain confidentiality, possibly even a covert relationship with a person who is assisting CIA and the government.

GREEN – Special access programs. I think this is a green light because it identifies that there are special programs that do require an extra particular attention to the classification. I think the 5 years renewable clause is a good one. I think that requirement does make it necessary to think further about particular programs.

GRAY – The Order draft forbids reproducing a top secret document with some exceptions. I can picture the head of my agency picking up a top secret document from the White House, coming back to CIA with the requirement to implement some action which might require going off in seven directions at one time. I find it hard to imagine his secretary not going to a Xerox machine and starting the process. I just don't know how that will work.

GRAY – I find there is some dovetailing but there's still some confusion to resolve as between the classification/declassification procedures and requirements of the new Executive Order and the Freedom of Information Act. At times it seems like one is getting it from both sides. As I go into FOIA and as the requests kept coming in, we noted a slight drop in the early 1977. We thought there's a light at the end of the tunnel. It turned out to be an on-rushing train with more requests. So the relationship between the two is a gray area from my point of view.

These are some of the areas that I have viewed in my color coding. What *is* the bottom line of the new Executive Order? It is an Executive Order that we can live with. The positive aspect is that we're going to have to focus attention again on what we're classifing – move away from an automatic process and go back to a through process.

The review process and the reduction in permissible time during which an item may remain classified from 30 to 20 years, poses a few problems. Parenthetically, in semi-jest, I wonder wherther there will be anything left to declassify in 20 years what with the increase in the number of FOIA requests. In connections with compliance with the Executive Order on declassification and compliance with the requirements of the FOIA one notes that it's rapidly becoming an expensive proposition. I would hope that as we proceed with all this, that the public becomes aware of the fact that it's costing the *taxpayers* a lot of money. What Congress projected in the FOIA to cost the first year in all of government was in the neighborhood of $500,000. Last year CIA's costs in salaries alone were over 2 million. The Department of Justice expended something like 14 to 15 million. Department of Defense was well over 4 or 5 million. It's a very expensive thing.

When an individual writes a letter to me under the Freedom of Information Act, it is costing the taxpayer an average of $540 per request. It's an expensive proposition to locate documents in a compartmentalized agency and to review those documents with enough expertise to make sure you are not giving away any information that must be protected in the national interests.

Before I conclude I might comment on some other aspects that I think we need to look at. The new Executive Order is concerned with making information available to the public and in being open. I believe, on the other hand, that we have to tighten up some other things. Of very serious conern to the agency right now is the rapidly increasing number of people who have worked in the intelligence community who want to go their way and want to do it by writing a book and by violating the secrecy agreement. Court decisions, as in the Snepp case for instance, are being watched closely. I would hope as we build the new Executive Order and as we are open under FOIA, that the Congress will become aware of what laws may be needed to protect some things.

Another aspect to consider is that even the new Executive Order still tends toward classifying information in a world war period. Perhaps we ought to look at some things that may need protection where foreign

policy or national defense are not related. I have several good examples of the kind of things I mean.

For example, the FBI released under the Freedom of Information Act – because they could not protect it – the Agent Handbook, "How to Catch a Bank Robber." The requestor was an inmate at Box 1000, Marion, Illinois. Fortunately, the warden intercepted it. Needless to say, there was one very mad warden. However, it has been released and 25 or 30 copies, have gone basically to various federal penitentiaries around the country.

The CIA received a request for a document, "Ten Ways to Murder an Individual Without Leaving a Trace of the Cause of Death." Now, *you* would say you wouldn't give that out, certainly wouldn't give it out to your neighbor. The document turned out to be a 1952 or '53 document that was submitted to the agency in case we needed it for some reason. On examination if was found to be essentially chemical formulae that any good graduate chemistry student could come up with; it's 22 years old; and it doesn't qualify for classification. We had to release it. (Ed. Note. It was learned subsequently that the request was acutally denied on the basis of a potentially adverse effect on the public. CIA was uncertain of the outcome.) Things like that bother me to have to put them in an envelope and mail them out to the public. We have a number of FOIA requests for documents on how to develop certain explosive devices, techniques from World War II, guerilla type warfare. These are things that I think we ought to be protecting, too. There are not too many laws or too many ways to protect the release of such information. The Drug Enforcement Agency tells me that one third of all their FOIA requestors are drug pushers and they're afraid they're going to lose some of their agents some day because of an FOIA request.

There was another the other day in which an inmate of a federal penitentiary wrote and asked for the blueprint of the penitentiary. The first government agency turned him down. The second one sent them. We had another very mad warden.

We recently compiled some information to go to Congress suggesting some amendments to the Freedom of Information Act because of some loopholes, as we viewed it, requiring release of more information than we really believed appropriate in certain areas. We can't meet the FOIA time deadlines. OMB could give us no encouragement so we have gone in to Congress in our annual report under FOIA and privacy pointing out some of these problems. But, the privacy and freedom issues in Congress are very emotional ones, and the trend today is for still more openness and I think that's the basis for the Executive Order is more openness.

In summary, I think the bottom line represents progress in the new Executive Order. It also represents considerable difficulty for an intelligence agency that needs to protect an awful lot of intelligence assets. It will be, for us, a matter of learning to cope. When you come right down to it, ours is a free and open society, and I would be concerned if it were not. So the fact is that we have to learn within CIA, for example, to adjust to an open society, even with the obvious difficulties it poses for us. I think we can do it, and will continue to work towards its furtherance.

THE NEW DD FORM 254

Marilyn Griffin
Naval Coastal Systems Laboratory and
Richard G. Butala
Hughes Aircraft Company

Summary of Presentation

Ms. Griffin covered salient points of change calling especial attention to a few of the numbers needed, what they meant, and where to find them. They are as follows:

PIIN – Procurement Instrument Identification Number. This six character, alpha-numeric designator identifies the user agency of the Prime Contracting Officer. It is the first part of the contract number found in block 3a. The catalog of these numbers and which agency is represented by them is contained in Annex N of the Armed Services Procurement Regulation. An example is N00019-identifying the Naval Air Systems Command of the Navy Department.

FSC – Federal Supply Code. This number is newly required and is five characters; numeric for a manufacturing facility and alpha-numeric for a non-manufacturing facility. The number to be used on DD Forms 254 is the one assigned by DISCO and is contained on the mailing label used in transmitting the *Industrial Security Manual* and the Industrial Security Letters (there are facilities having more than one FSC number). One should ask for the number when requesting verification of facility clearance or from the company/organization when written, telephone, or personal contact is made for any reason. *Record* it for

contractors with whom you do business regularly. There is no available consolidated list.

DODAAD – Department of Defense Activity Address Directory. This number should be included on any newly issued DD254 in its proper place (item). If it is not it can be learned from the published Directory available through DDC as DoD4000.25D. (Ed. Note. However, if the user agency has failed to include the information in their DD254 to you, let then worry about it; note "Not Provided" in block).

It is recognized (and complained about by some) that these numbers are not related to classification specifications. They *are* related, however, to the management of the system with computer aid so that, eventually at least, a contractor need not be embarassed by having to ask for an update of the DD254, for example. The system, as one understands it, should help the contract or despite the minor bother of adding some numbers to his sub-contract forms.

Then Mr. Butala highlighted some of the other changes with example of a DD Form 254 that Hughes Aircraft might prepare. Among them were:

- The respective paragraphs have been numbered differently from the old 254 because of the decision to number the "Date to be Completed" column as number 4.
- The access requirements have been elaborated. IPO (International Pact Organization), Special Compartmented Information (SCI), and Classified Automatic Data Processing (ADP) are included and defined in Change 1 to the *Industrial Security Manual.*
- A signature requirement has been added to a certification statement that "guidance is adequate and current." It is expected that *the* person really coordinating classification will be one who's name will appear and who will sign. (Ms. Griffin had commented that she would hope that it would be, for example, a Security Classification Manager so that the guidance could be coordinated).
- A decision on the form in which guidance is to be, is required. Providing it separately – as in the case of classified guidance, for instance, is recognized and included in the preliminary statements/selections.

Mr. Butala noted that all concerned would need to put on their "Cooperative hats" and that with those no insuperable problems would exist. At the conclusion of his remarks, Mr. Robert Green, from DLA offered a few comments regarding its need for the FSC and DoDAAD numbers. He noted also that they were discussing instructions (he said that it was unfortunate that none were distributed when the form was issued) to user agencies and the form in which they should be. He said that there would be an Industrial Security Letter out soon that would explain further some of the aspects on which questions had been raised – both from the user agencies and contractors. He commented that the instructions also could go into the Industrial Security Regulation (Ed. Note. one would assume they should) and it is binding on all agencies participating in the industrial security program. He finished his remarks by noting that the last item for potential instruction was a re-issue of the handbook on writing classification guidance – done initially "during the George McClain – Don Garrett regime at OASD." It is being considered also as a nucleus for instructions on the proper use of the 254. He closed saying that one should view the new DD254 as an evolutionary process and that they expect to have all the information needed to use it properly available in the near future.

THE SIGNIFICANCE OF CHANGES TO THE INTERNATIONAL TRAFFIC-IN-ARMS REGULATIONS

Bernard Femminella
Director, Office of Munitions Control

Introduction

The Office of Munitions Control of the Department of State, is tasked to control the export of arms, ammunition and the implements of war, as you know. As you will remember the authority to do so is the Arms Export Control Act which was passed in June of 1976 and under the legislation we promulgate the International Traffic in Arms Regulations (ITAR).

The Office of Munitions Control is not physically in the Department of State; it's in Arlington. There are about 29 persons to manage a kind of a mass production of license applications of all kinds. About 26,000 actions were processed last year, covering exports of hardware, technical data, temporary exports, advisory opinions and all of the transactions that you all have with us.

What is it that we control? We might remind ourselves. The term arms, ammunition and implements of war is kind of amorphous; one needs some further definition of what such things are. The definition is found in the U.S. munitions list, as you are aware. It's not a *catalog* of things you will recall. Rather it's a *list of categories* of things. So that starting with firearms, it means *all* firearms – from target pistols right up to submachine guns and machine guns. The same holds, of course, for combatant warcraft, aircraft, any military aircraft, *etc.*

We are at this moment in the process of updating the munitions list. I believe it was last fall, we sent out a flyer saying that we were going to update the ITAR and the munitions list. Some of you, at least, would have seen it. We are still in process on the updating. Such matters take a substantial time to complete. You readily recognize that policy – as, for example, President Carter's announced policies – cause questions to arise. Another aspect of that point is that the Executive Order that establishes the responsibilities of the various government agencies in this field requires that any change to the munitions list shall have the concurrence of both the Secretary of Defense and the Secretary of State.

Another point for recollection is that *nothing* manufactured in the United States – whether an aircraft carrier or a jar of peanut butter – can be exported without some kind of a license. If it's on the munitions list, the Department of State controls and licenses the product. If it's not on the munitions list, its export is controlled by the Department of Commerce.

As some of you may not know, the Department of Commerce has two kinds of licenses. They have what you call

- a validated license (which is indeed a piece of paper) and,
- a general destination license.

The latter is nothing more, in effect, than a list of things that can go to almost any country in the world without any kind of a license or a piece of paper.

As a consequence, if we take something *off* the munitions list, it has to go *on* the Commerce list. So, one of the problems that we're facing right now is; where does what we take off the munitions list fit into the Commerce list? There's a lot of hang ups there and when we get those things straightened out, then maybe we'll get a new munitions list on the street and then a new ITAR.

The ITAR

Now let's talk to the ITAR. It starts off with the munitions list and then in the next chapter talks about registration. Everybody in the United States who manufactures or exports an article on the munitions list must *register* with the Department of State and registration requires payment of a fee. This requirement poses a small problem. Many business people in the United States who like to do business don't like to be "licensed" as they view it. It isn't the fee – it is very small, as you are probably well aware; about $125 a year. The only purpose in the requirement is to produce a list of businesses that are registered. The list is established because the Mutual Security Act of 1954 (the "Munitions Act") established a requirement that there be one. I've been with the Office of Munitions Control for three years now and we do nothing with the list except maintain it and certainly nothing that would cause any reluctant business person to be concerned. When something is added to the munitions list, obviously every manufacturer of the item in the United States must register with us. This is another factor holding up the publication of a new ITAR.

Part 123 of the ITAR talks to the licensing program and it lays out very clearly what you have to do to get a license to export either hardware or technical data. One of the newest things that the Carter Administration added to the ITAR was the requirement for prior approval before you can make a presentation or proposal to induce a sale for 7 million dollars of significant combat equipment for use by a military force abroad. That's practically the whole regulation and it's all one sentence. I'm told that many of you face problems in that area. However, no two companies have exactly the same problem so there are essentially no general suggestions to make. Probably this requirement will be the only new addition to the licensing section we'll do except to do some smoothing of language in the ITAR.

Part 124 deals with technical assistance agreements and manufacturing licensing agreements. In the last year, within the government itself, we have become much more stringent about licensing or approving manufacturing licenses agreements. In May 1977 the President's policy statement said that there would be no co-production of significant weapons. The exceptions, of course, were the NATO area, Australia, Japan,

and New Zealand. As a result, we find that in the last two fiscal year quarters we have had to reject many more requests for licensing arrangements and it looks like that's going to be a trend. Your past president, Mr. Richardson commented that it's difficult to do business in the present climate. It's quite possible that this policy, affecting co-production or what you call the licensing agreements, is the problem behind his comment. It appears, however, that there will be fewer and fewer approvals in the future.

Section 125 of the ITAR covers the exchange of technical data. All of you know that the term "technical data" is a very, very broad term and covers *information* regarding items on the ITAR. A license is required. You can't discuss technical data outside the United States nor in the United States to a foreigner without a license. No change in that section is contemplated.

The newest section of the ITAR that you might find interesting is that on enforcement procedures. A violation of ITAR, under the Arms Export Control Act, was a criminal offense and penalties were on the order of $100,000 fine and two years in jail – that's for *willful* violation of the ITAR. Well, it's very difficult to establish willfulness. Many people may do things in good faith but nonetheless violate the ITAR. It is not our intent to throw anyone into prison – unless it's a deliberate thing like the gun-runners, for instance. We go after the gun-runners but, the manufacturer that ships 120% of lots of spare parts for aircraft instead of the 110% he's allowed bacause of some administrative aberration in the organization, is *not* the manufacturer we desire to send to prison or whose production we want to stop.

However we *have* adopted a rule which says we can debar a corporation from enjoying the rights of export if there is other than a criminal violation. We are clearing the use of Department of Commerce hearing examiners in order to administer and implement that section of the regulations.

The only remaining part of the ITAR that may be of interest is part 130. You may recall the scandal of a couple of years ago about people paying bribes to sell aircraft. Since then we adopted a regulation requiring a disclosure statement for each $100,000 license application. It must set forth any political contributions, and fees or commissions that you may have paid relating to the contract. We defined a political contribution as a contribution that is $5,000 or more and a fee or commission as a payment of $100,000 or more. You haven't paid a commission unless it's $100,000, and if you do, you must disclose that. Further, if you pay a commission to a fellow abroad, he must disclose to you and you to us whether he's bribed someone – and we get such reports. That's because there's a very interesting point here. There's no rule against paying a bribe but you've broken the law if you don't tell us.

Futher on that point, at the end of every quarter the law requires that we inform the Congress. So, we take the disclosures, package them neatly and send one copy to the Speaker of the House and the other copy to the Chairman of the Foreign Relations Committee. We've been doing this now since December of 1976. I'm not sure that anyone has yet been called to task about any such disclosure, but that fact notwithstanding, that is the regulation and the law. One can't count on there not being any questions in the future.

Commenting on the disclosures, I have found in the last year or so that people are over-cautious. Company X will report that they have paid no political contributions but they did pay John Doe in "Country A" $5,000. They didn't have to do that; the requirement is that they report $100,000. What happens when one reports a payment of any sum one triggers the section of the rule that requires reporting what John Doe in "Country A" did with the money. If the report merely had stated that there were no payments of $5,000 in political contributions or payments of $100,000 in fees or commissions no further comments were required, and the report could have been signed and sent.

These comments have covered the charges to law and regulation that may be of interest and have an effect on some of you.

Questions and Answers

Question: During the past year there has been much comment in the media to the point that presentation of technical papers at professional associations might be considered a violation of the ITAR if the subject matter could be considered a part of the munitions list. Would you comment on that, please?

Answer: Absolutely true! If your subject matter is technical data, you need a license to present it to a corporation, a foreign government, or even an organization like this.

On the other hand, if the presentation is conceptual for example when Einstein set forth his theory of relativity he did not have to get a license to present that in a public forum or overseas; but when someone

else took his concept and created a practical application for constructing an atomic bomb, *that* was controlled. Textbook information is not controlled. However, information that helps in building a rowboat or whatever, that is covered by the munitions list, is specifically controlled. If you plan to talk about a new discovery on a radar and what wires you have to switch to make the beam turn right corners, then a license is required.

Question: When reporting payments at $100,000 or more there is a requirement to name the person who receives the payment (according to Section 130.22). When one names a person, considering the terrorist activities in various countries, there is concern about whether we identify that person as a target, or as a hostage candidate. Since these letters do go to Congress, do you have information about what happens when they get there?

Answer: When we notify the Congress, we do say that the corporations have required or requested confidential treatment of the information, and that we would appreciate their giving confidential treatment to transmitting letters as well. You have not seen any such in the *Congressional Record.* That is the means by which the Congress would make something public. Although corporations should request Confidentiality in their submissions, we put a blanket caveat on our submissions notwithstanding the failure of a given organization to request such treatment.

Question: Some confusion exists respecting approvals of export by one department government then later retracted. Two instances came to mind. One was the Oshkosh Trucking Company, I believe, which had a contract to provide a number of their vehicles to Libya. Later the approval was rescinded.

A second was the sale of the Control Data Corporation computer 7700 to Russia which was later disapproved also. Commerce, according to media, had approved both and then later had retracted the approval. Would you offer comments?

Answer: I know of only one of the cases. Remember that licenses are issued in furtherance of world peace and the defense and foreign policy of the United States. That's by law. The Department of State as you know is responsible for our foreign relations & policy. It's not actually in the *control* business. The whole licensing program, while it looks mechanical, is a tool of foreign policy. We can, as you very well know, pressure certain governments to do things or pressure them to not do things.

Turning to the Oshkosh Case. The trucks proposed for sale were not on the United States munitions list. They were under the general destination list, but they *were* going to Libya. United States foreign policy is not to help Colonel Kadafi in any way at all as long as he maintains close ties with the Middle Eastern terrorists. He's a thorn not only in our side, but also in the side of the Israeli, the side of the Egyptians, the side of the Lebanese, and the side of the Sudanese. He is a thorn in everybody's side as long as he continues his support of terrorists.

Our foreign policy is, as I said, don't let him have a thing – nothing. The trucks in question were tank transport vehicles, but they were in the general destination category. The Department of State had asked the Department of Commerce to move those from the general destination category to the validated license category and then make them unavailable for export to Libya. In the process of doing that, Oshkosh unfortunately got caught in the transition, I must admit. They were told about a year ago that the Department of State would not sanction the export.

Question: The question concerns prior approval, perhaps you can provide some clarification. Is prior approval needed to discuss "things" with foreign visitors, provided we do not discuss technical data?

Answer: The regulations say, as I mentioned, that you may not give a presentation or make a proposal that is designed to induce a sale. This is a very, very difficult area for us to deal with, too. What we've told many companies is that if they have been dealing with a given country on a particular program or list of programs, send us the information – if the talks began before September 1, 1977.

It's very difficult to say at what point one approaches violating the regulation. You may not, of course, give price or availability. That's established in the regulation. You may not give technical data, as you infer, but then that too is covered. What you can't do is probably beyond either my imagination or my ability to recall; what you *can* do is apply for prior approval if there is an upcoming program or apply for a technical data license and that also is prior approval.

Question: As a follow on question, considering that time is of the essence since we're competing with foreign governments as well as other US manufacturers, how long does it take to get a prior approval?

Answer: A request for prior approval is treated as a request for an advisory opinion on a license to ship hardware. It's given the same trip around Washington

for approval and constitutes a moral commitment of the government to license the subsequent hardware, and you may have realized that in fact if there has been a prior approval as you outline and there is a sale, and then an application for license is made, within the six months of the prior approval, you get a license in 24 hours.

Remember that our commitment is a moral one and that is dissipates with time. Remember also that it dissipates with headlines as well.

Question: Could we change the circumstances of the question you just answered slightly. If a visit has been approved on a classified basis, and authorizes the disclosure of, say, U.S. confidential information, it would authorize the disclosure of technical data. When we are disclosing technical data, it's likely that the three P's – price, performance, and probable availability – will be included in one way or another in classified discussions. What problems or authorizations are likely in that case?

Answer: In the case of a sponsored visit you would be allowed to talk performance but not price and availability. For that you would have to come in ahead of time. That may sound bureaucratic but it's because the service that gave you permission to talk about classified data, is not the service that is going to make the final decision on a sale.

Comment: You may not know that most of these visit authorizations are received by the contractors the day before the visit takes place, having been submitted by the foreign government through his embassy to the foreign liaison office of the military service involved. We would not have time to request prior approval.

Response: However, the rule still holds.

Question: The question of time, as it relates to repaired items, seems to be becoming a problem. The Commerce Department controlled items are allowed to be re-exported after repair under a general license even though the original export required a validated license. Is there such a provision under OMC?

Answer: We don't have a general licensing program in the Office of Munitions Control. We tried to get one for some items on the munitions list but when we spoke to the staffers in the House International Relations Committee, we were denied.

Question: Are there any other creative ways to assist a customer in repair turnaround?

Answer: Not really, You've just got to go through the same process. You have to understand the difference between Department of State licensing program and the Department of Commerce licensing program. The Department of State is in the control business and Commerce is in the promotion business, and there is a big difference.

ITAR CHANGES THAT IMPACT ON INDUSTRY AND THE ECONOMY

Dr. Hylan Lyon
Manager, Advanced Planning, Texas Instruments

Most of us in this room wrestle with the day to day issues in export control, government classification, information privacy and a number of other implementation problems. During this daily wrestling match, we try and cope with the impact of a myriad of procedural changes; Office of Munitions Control circulars, and commodity control list definitions, to mention only two. In addition to these procedural problems, in export one faces also the ever changing criteria of case by case reviews. These are compounded by a steadily increasing number of spokesmen for one or the other aspect of national interests in security or other policy. The two other participants in this part of the program have highlighted many of the issues and have explained to us how they have accommodated to the present situation. I intend to philosophize a little more than they have and try to give you my impression of some factors that will be or are creating change, either in policy or practice. This approach will be wide ranging but we shall focus on the ITAR aspect of export control and technology transfer.

When we talk about ITAR we are talking about international business and the international market place. In general the international market is viewed by the western democracies in an ideal sense as a free competitive market. But, in a practical sense it is a market full of government intervention and non-tariff barriers managed through a number of macro- and micro-economic instruments. Even so, at the policy level our basic U.S. position is to remove unnecessary restraints to trade, forestall protectionism and as a general principle reassert our commitment to more liberal trade.

Several of the interventions which appear justifiable are associated with restraints, controls or outright embargos on trade in military items or supporting technologies. The ITAR (the *I*nternational *T*raffic in *A*rms *R*egulations) is an executive order issued by the

President by virtue of authority vested in him by Congress in the Foreign Assistance Act of 1961. The regulations are published in the Federal Register, as title 22 of the Code of Federal Regulations. The President's authorization for control is in futherance of world peace and the security and foreign policy of the United States. Under ITAR there is a munitions list of articles which will be denied to communist countries. These items may be approved to non-communist countries if the criteria are satisfied.

To give you a feel for the size of the arms export problem in relation to overall trade, consider that in 1976 U.S. exports totaled 115 billion, 77 billion of which was manufactured goods. This can be compared with the approximately 9 billion figure representing foreign sales of munitions list items, either directly or through Foreign Military Sales (FMS). FMS are the special cases where the U.S. Government acts as the purchasing agent, *e.g.,* the U.S. corporation sells to the U.S. Government which in turn sells to the foreign government. During 1976 the U.S. ran a trade deficit of 27 billion. Therefore, military sales are roughly 12 percent of all manufactured exports or equal to one third of our balance of trade deficit. The "bottom line" is that military sales are a significant amount of U.S. exports with a comparable impact on jobs and industrial production due to arms sales and GNP growth.

The Munitions List which is the key to this process of control has not been seriously reviewed since 1969. For example, mustard and ketchup were removed some years ago, and I have heard that bayonets are being suggested for deletion. In general, nomenclatured items; that is those items with AN/ numbers, are major items on the list. One of the major factors creating pressure for change is the shift in the technology base which now supports and is used in both commercial items and military items, both included in U.S. exports. The example I will use is the integrated circuit whose initial development was spurred by the requirements of the Minuteman missile; but now the Defense Department represents only 7 percent of the integrated circuit market. As a result, primary application of integrated circuit technology is found in consumer goods. This shift in primary usage of leading technology causes a number of problems associated with defining the security related issues in U.S. export control.

This phenomenon has resulted in the term "dual use" goods and technology. The issue of dual use goods surfaces in three ways. First is the problem of technology transfer of critical defense technology associated with commerical non-military items. These questions surface primarily in the licensing process in the Department of Commerce since the commodity itself is not on the munitions list. A second way this issue surfaces is in items of lethal/non-lethal distinctions where there are a number of military nomenclatured – munitions list items covered under military sales – that are not used in direct support of offensive or defensive military actions (such as C-130 transports, nomenclatured air traffic control radars, or military construction). The third way the issue emerges is in military co-production of end items. This may result in the establishment of a foreign competitor in such a way as to have a long term impact on the U.S. economy.

Several new trends in the way end items are related to technology and support systems have developed. To my way of thinking, the modern high-technology product becomes less and less susceptible to reverse engineering. Therefore the technology, capability or "know how" to produce is becoming more divorced from the end product. My first reaction to this trend was to say that this should make the export problem easier. We could simply sell the products and not the know-how. That is too easy, because what happens as a result is that the know-how is requested quite frequently as part of the package deal, either as *a priori* condition of offset or coproduction or as part of the support hardware or software and test equipment. Therefore, a reality in this type of business is that explicit requests for supporting technology packages will become a *predictable* part of major overseas sales.

There is an intriguing question inherent in this topic; one that I have never seen addressed. It came up some months ago when I did a short stint as a consultant to DDR&E related to the industrial views on export control. I reviewed several thoughtful letters from industry which had been received by DDR&E, the White House or the Department of Commerce. One of the comments ran like this, "why isn't the Industrial Security Manual adequate protection for the national interest?" This seems to be a legitimate question since there is an article in the ITAR related to the control of export of classified information (data and equipment). The thought kept recurring to me; that if "critical technology" were defined properly, as proposed in the DoD guidelines of the 26th of August, there may be only a small area of information that exists outside of these national security classification criteria. If this is so, perhaps we have an *implementation* problem not a *policy* problem. I would like

to share the results of my thought process with you today.

The DoD interim guidelines published over Secretary Brown's signature refer to critical technology as the classified and unclassified nuclear and non-nuclear unpublished technical data, whose acquisiton by a potential adversary could make a significant contribution – one that would prove detrimental to the national security of the United States – to the military potential of such country. Consider the classification criteria in the Executive Order Draft state:

> "Information may not be considered for classification unless its disclosure could reasonably be expected to (4) aid a foreign nation to develop or improve its military capability, or . . . ."

The classification requirements state that information shall not be classified unless an original classification authority determines both:

- That the information falls into one or more of the criteria, such as 4 above, and
- That the disclosure of such information could reasonably be expected to cause at least significant damage to the national security."

Simple linguistic analysis of these two texts would lead you to the conclusion, that, at this level of detail, the requirements and criteria for classification as national security data or as critical technology are the same.

The problem lies in the fact that both export control and national security procedures recognize that an insensitive application of these requirmeents and criteria would have adverse impacts on several other aspects of the U.S. economy. These competing objectives are considered as valid and as protecting national security.

The Executive Order states that as a general policy in deciding whether information requires classification, the classifying official shall consider both the public's need for the greatest possible access to information and the national security need to protect certain information. The Order also has certain prohibitions. One of which is:

> "(3) a product of independent research and development which does not incorporate or reveal classified information to which the producer or developer were given prior access shall not be classified under the Order until and unless the government acquires a proprietary interest in the information. The Order shall not be construed to impinge upon the provisions of the Patent Security Act of 1952."

The interim guidelines state that Defense Department must discharge its concern over national security without restricting U.S. trade and exports any more than necessary. There are few other statements in the interim guidelines which can be interpreted as explicitly reflecting the need to resolve the conflict between competing demands of the U.S. economy and control of exports for national security matters.

At first blush, one might say that the laws on control of exports are significantly less lenient than the security classification criteria with regard to information control, and one might add that the criteria for implementation are less clear and understandable – others have said as much. Yet, if one recognizes that the new guidelines recommend a shift away from a product control philosophy to a technology control philosophy, and if one reflects on the definition of critical technology as opposed to non-critical technology, one might agree that if the approach proposed in the Brown memorandum *can* be implemented completely, significant positive results could be obtained.

The Presidential Study in the final stages of review should give the critical technology approach a period of time to prove feasibility of implementation. One characteristic of such a feasibility demonstration will be the development of a close structured relationship between industry and DoD. Some rather interesting developments in this regard have occurred with the formation of nine critical technology expert groups by the industrial association to work with USDR&E. If these groups are successful, their results will be utilized and communications will improve. As a result, industry should know what the ground rules are for export control, both in concept and in practice, because train of logic will lead back to legitimate and understandable criteria. More accountability for positions taken and predictability of results should occur.

Why have I stressed technology transfer under an ITAR discussion? You should be asking me "why isn't this more appropriately a topic for discussion under Commerce Department controls?" There are two reasons, the first, which I covered previously, is because critical technology comes close to information that is assigned a security classification in which case

ITAR is the controlling regulation. Secondly, because the coproduction of military goods with our NATO allies will generate a host of license applications for technology transfer under ITAR. The Harold Brown guidelines are equally applicable to these situations as well as the commercial situations. In fact, the experience of Texas Instruments, Inc. has been that the first changes in our environment due to the Brown memorandum were conditions placed on ITAR license approvals associated with restrictions on the transfer of critical technology.

In conclusion, I would like to leave you with the impression that it will be some months before the technology transfer issue under ITAR becomes understood in an operational context. If industry continues to work closely with DoD in understanding and communicating each others concerns, I feel that it will be possible to expect positive results. The effect would be to strike a balance between the growing need for the U.S. to increase exports while at the same time to protect national security.

Edward Silver
Manager, Government Liaison,
Hughes International

Initially, I would like to limit my discussion primarily to the problems created by recent changes in the requirement to obtain prior approval. But before I turn to the changes and problems as I view them, in fairness I should comment that some of them at least could very easily be placed on the shoulders of industry. There was a very diligent attempt to seek industry comments about the proposed change prior to its becoming law. So, if there are problems, industry must recognize that part of them are their own fault for having failed to take advantage of the opportunity to provide comments and offer suggestions.

First, in connection with identifying problems, I would like to use what I call the leap frog system for control. Under that system we find what forms of control pertain to a given category and how and when ensuing forms of control are imposed. It appears to me that there are three or four tiers of control being exercised by the State Department today and one leap frogs from one to the other.

The first tier would be munitions control items that, for a lack of a better term, I will call insignificant combat equipment. It's not significant combat equipment like a tank or an airplane but yet is on the munitions list. For example, by determination equipment such as bayonets and silencers are not significant combat equipment. On the other hand, communications satellites, by determination, are significant combat equipment. You can see that the term can be a little misleading in itself.

We have attempted to learn what the official definition of significant combat equipment is, or what the definition of insignificant combat equipment is. It appears that there isn't one. One learns which is which by examining the munitions list for asterisked items. When there are "stars in your eyes," you know you've found gold – or another hang-up.

Now is the time that one begins to enter the arena of leap-frogging. If one starts with a piece of equipment originally *not* "significant combat equipment," and all of a sudden it *becomes* significant combat equipment, one potentially enters a new "ball game." Such an item may become a piece of "major defense equipment." Let me remind that each time an item enters a new category or has a new title, a ominous sound of dough may be vibrated through the Congress. To go from *significant combat equipment* to the category of *major defense equipment* is a tier. For that there is a definition; if the U.S. government has invested 50 million dollars in R&D or 200 million dollars in procurement on a significant piece of combat equipment, it is automatically major defense equipment.

Now, we have leap frogged to the third level. What this means to us now is that if we have a piece of major defense equipment and the sale is for over 25 million dollars, and the sale is proposed to a non-sacred circle country – by "sacred circle" I mean NATO, Japan, Australia and New Zealand – we just lost the opportunity to sell. It will have to go FMS, even when the equipment is not being currently procured, or not necessarily being proposed for procurement in the exact configuration that the U.S. military service purchased it.

There is a special significance attached to the level of "major defense equipment" in that it requires a special report to Congress. Anything over 7 million dollars must be reported. The 30 day lead time on such cases makes potential sales that much more difficult to consummate.

There are also some other significant elements relating to major defense equipment. When one applies for a license in such a case, one must include: a copy of a DSP, a signed DSP-83, a copy of a contract or letter of intent, a clear statement of the dollar amount, a clear statement of the end user, which the DSP. 83 would probably in itself describe, the item capabilities,

and something very interesting for us – the number of United States persons necessary to support the exported equipment abroad. That is a difficult question to answer because it is dependent on the ability of the foreign customer to assimilate and care for that equipment in his inventory. Certainly, we can project that for the first year or two, but beyond that, it is extremely difficult.

Now, consider another facet; that of significant combat equipment and prior approval. Mr. Femminella discussed what was needed in prior approval. I call the requirement P^3 – price, performance, and probable availability. However, we are able to enter into things called "preliminary discussions" to ascertain market potential. The regulation goes on to establish that requirements apply when one is selling "significant combat equipment" of a value of seven million dollars or more, and it's intended for the armed forces – whatever that means. By way of a point, sometimes we find that when selling to a foreign government, the government *is* the armed forces. What we might be selling might be for a very standard commercial application, such as a communications satellite, for example. However, the *procurement* organization is the armed forces – they run the telecommunications system.

So, we take a little umbrage over the term "intended for the armed forces." It would seem to me that "intended for a military purpose, or its use in some military application" would be better by far. I recognize that probably our military is one of *the* biggest users of the Bell telephone lines that exists, but nonetheless I feel that the terms are somewhat conceptually and specifically confusing.

A third related point was the requirement that there must be an export of either hardware or data to make this item qualify as needing prior approval. In this context, we can satisfy the requirement by certifying that we did not make any presentation or propose anything requiring prior approval. Or, we can satisfy the requirement in three other ways.

- Ask for and obtain written approval
- Obtain a license to export technical data that describes equipment in question
- Obtain a license to demonstrate the hardware to the armed forces.

The last brings up an interesting situation. Many times in the past we have obtained demonstration licenses where the demonstration was not necessarily to the armed forces but rather to prospective licensees. The need for prior approval would not seem to have existed if we obtained a demonstration license only to a civilian organization instead of a military organization.

Returning to the P^3 area, there are some problems. A question I would raise is, if we give price and performance but we don't give probable availability or we give probable availability and price, but we don't give any performance, have we violated the rule? For the answer to this (we don't know exactly) we went back to the intent of the regulation and tried to ascertain if the disclosure of pieces of the information would provide a sufficient basis to make a decision to purchase.

Price, performance and probable availability is a nice cueing device, but I don't think it's a complete answer. I think the ultimate answer lies in whether or not we have actually provided sufficient information to make a decision to purchase. However, that approach is causing our people some concern and we are attempting to resolve that. For example, the standards for data. Sufficient information to make a decision to purchase would vary by country. One country would require a detailed life cycle cost analysis where another country would simply accept the reputation of the company proposing it. What's needed would vary with the equipment and it would vary also with any prior briefings that had taken place earlier than 1 September 1977.

Further, we find that Canada is sort of a special case. Now, you will recall that there were four tiers that the State Department controlled . . . the less than significant combat equipment, significant combat equipment, major defense equipment, and, newest, the prior approval requirement. We find that, because of the exemptions, we can go into Canada and give technical discussions – presentations on an unclassified basis without prior approval – without any license, and we can disclose design and engineering. We can disclose just a heck of a lot of very detailed technical information in Canada but when it comes to the point of price, performance, and probable availability, we have to go back to the State Department. Not true? It's the way it's written.

Comment by Mr. Femminella: Prior approval exists in the exemptions.

That's an interesting point that we had not learned. The comment pointed out that the exemption that Canada enjoys because of the way it appears in the ITAR, also satisfys the prior approval requirement.

Another problem relates to technical data. If the tech data is *almost* the same but *not quite* the same, or if the demonstration hardware is the *same hardware* but it's for a *different purpose* or *application,* we feel uncertain about a decision that a previously granted license to export that data or hardware satisfies the prior approval requirement since the purpose of using the hardware has changed.

One of our biggest problems is trying to translate into legalese. If any of you ever have been involved in writing a license and a technical assistance agreement, you realize that lawyers have a special jargon. Price, performance, and probable availability are not in their vocabulary. So, if one takes the word *price* when one translates price into an attorney's jargon used in writing a license and technical assistance agreement, we have had to presume it translates to royalty rates.

When one takes the word *performance,* we're at an absolute loss to translate. We have come to two conclusions. Either it means the license grant, or it means performance of the hardware that is the subject of the license – recognizing that all licenses written do not cover hardware. Sometimes we license the use of data and the foreign customer uses that data to design his own hardware. So, we're at a little bit of a loss on trying to translate how performance applies in a given case.

Then, *probable availability.* We think we have that translated and solved. We think it's called "term of the license," but we're still not absolutely certain. So, I think, those words were poorly chosen as applied to license and technical assistance agreements. If one hasn't bridged the gap from the requirement to obtain prior apporval for sales of hardware, to manufacturing license and technical assistance agreements, one should do so quickly. The regulation covers both; for manufacturing license and technical assistance agreements, there is no 7 million dollar threshold – all manufacturing licenses and technical assistance agreements are covered.

Now, where is all this leading us? Is there a concern? In comparison with 1974 sales of hardware – arms exports, not including construction or services – the United States has been declining each year in comparison with European countries. It appears to be the interest of the President (and the Congress) to do so, what with the ceilings placed on FMS. In fact the ceiling for 1977 calls for a limit of 9.33 billion. That requires an 8 percent reduction each year. When that figure is compared against all the commitments for sales that are priority claims against that ceiling, plus the logistical support for prior sales, there is not going to be much room left for future FMS sales.

The United States is going to either have to remove the ceiling very soon or else we're going to find that there will be no new FMS sales and you say, "Well, how does that affect industry?" Recently, the Iranian government approached the U.S. Navy and asked for the sale of some frigates. The U.S. Navy responded that they could not honor such a request and, I think the reason was because of the ceiling. By the time the frigate sale could be squeezed under the ceiling it would be untimely considering their needs. Therefore, it was suggested that Iran go to the Netherlands and Germans.

We are still trying to follow that sale and trying to get our equipment on board a frigate that will be built in either the Netherlands or Germany. We find that our opportunities to sell support equipment on U.S. built frigates is much higher than it is, say, on selling equipment on Dutch built frigates. So far we predict the probabilities of a sale to be zero percent on a Dutch built frigate.

In closing, let me just say that there are several actions that the U.S. government seems to be undertaking that make it extremely difficult for contractors to operate abroad. First of all, they've hit us on income tax. Secondly, they've taken away our right to talk to the embassies, the MAG's, the ODC's via the Duncan letter and other letters. Third, they have imposed new requirements for prior approval – an approval not only from the State Department but also requiring coordination through the Congress – a very long and lengthy process. At the same time they're encouraging us to engage with NATO countries on something called rationalization, standardization and inter-operability. We seem to be caught in the middle of a "trichotomy" where one side's saying "Stop, don't go" and another side's saying "Yes, go," and still another is saying "Yes, if."

We suggest that the contractors be given a better shake if the U.S. government really is going to rely on us to do something to balance the export deficit that we have.

Questions and Answers

Question: Is it incumbent upon a scientist or an engineer to be aware of the contents of the munitions list if he or she is planning to deliver a paper or write

an article to make sure that it does not incorporate something on that list?

Answer by Mr. Femminella: Yes, it is. The requirement follows the principle that ignorance of the law is not an excuse.

Question: Is this regardless of whether he makes the presentation in this country or in a foreign country?

Answer by Mr. Femminella: Yes.

Question: There is a gray area in my mind. Perhaps you can clear it up. When a technical person prepares a paper to present at a symposium or conference, he or she submits it to the Office of the Assistant Secretary of Defense, Public Affairs for approval for public release. Having obtained that, it's now in the public domain. Where then does the State Department find its authority to require a license?

Answer by Mr. Femminella: It doesn't; that's exactly right. There is a section of the ITAR that exempts anything that's in the public domain. If technical data has been publicly released by competent authority in DoD no further approvals are required – that's in the ITAR.

Comment by Mr. Robert Behr (Air Force Systems Command Wright Patterson Air Force Base): Mr. Silver raised a point or question on the manufacturing technical assistance agreement license. Where does one put performance data? When it's included in the manufacturing license, it's my current experience that it's being put under the definition of product. In the opening definition paragraph A there is a column "Product". That column can be expanded to include all the performance data one needs when one applies for the license for a given system. I realize that one might not quickly arrive at that conclusion, given the language used in the Regulation and Forms.

Question: Regarding "public domain" type of information, if I understand correctly, isn't there a stamp that is affixed to information released to the public that says essentially that one must go to the ITAR if one is planning on foreign release; that the release is only for U.S. dissemination? Is that right?

Answer by Mr. Femminella: Any technical data that's in the public domain can be freely exported without a license.

Question for Mr. Femminella: There seems to be a question of how the contradiction between a growing demand by foreign governments for technical assistance agreements will be reconciled with President Carter's stand on limiting co-production. You made a statement that co-production licenses would be approved in fewer and fewer cases but Dr. Lyon says the demand is increasing. Can you speak to that, please?

Answer: Yes. I think the President's going to win in spite of foreign governments desires for additional technical data. With this President we're entering into an era of "turn licenses down," not issue them in mass production. It's become a policy of restraint and I guarantee you that the fact of the economic impact and many of the other things that were mentioned by speakers who followed concerning exports had been taken into account. Nonetheless, the incumbent President's policy is to limit the export of arms from the United States.

Colloquy, Mr. Russell L. Logan, Radar Engineer, Texas Instruments: I came to this meeting to clear some of the confusion from my mind; I've been consoled to learn that I'm no more confused than most people here. Very seriously, however, the definition of technical data is a *major* issue and concern in professional societies. The IEEE, for example, is frightened to death that if Mr. Femminella ever gets enough staff to handle these 30,000 applications per year, we'll probably all be put out of action. The concern, which has been touched on by others, is over the publication of technical information or papers. For instance, an engineer in the United States who submits a paper to the IEEE for journal publication now has to remember, I suppose, that the journal is internationally circulated.

The point comes to mind that if technical data is defined as I heard it here – namely that it's information sufficient to make a procurement decision – we're virtually unable ever to give that much information no matter how hard we try. If that is the case the, perhaps, technical data in the form of a paper that's an extension of some known principle may not be subject to such review and restriction. That is a question in my mind, however.

To cite an example of why I'm confused, recently an issue of the *Scientific American* went into great detail on coherent synthetic side looking array radars. Heretofore, that technology had been cloaked in secrecy; now it's in the public domain. Any average engineer in radar or electronics can take that article and other available handbooks and, through pragmatic application of standard engineering principles, readily tell you just about what kind of radar the world is capable of producing – free world or not.

Consider for a moment that professors, engineers, and scientists, are very prolific people who publish a lot of information. At this time, anything that is not

published is not published because either it's classified or it's company proprietary. Those two areas wouldn't be revealed in any kind of preliminary discussions in any case. In my view those of us in the technical world have a conceptual problem on what *is* technical data, and I still don't know. I would appreciate any guidance or clarification that one could get.

Mr. Richardson, Seminar chairman: May we try to clarify your question. Are you asking what is technical data, or are you asking what constitutes a decision to buy, or what constitutes information that would cause some potential customer to make an offer?

Mr. Logan: What I'm really asking, I guess, is what is technical data. I also offered examples of published information that I hope would be considered as outside the restriction discussed. If the definition of adequate technical data for procurement decision is viewed as the massive amount of data that we normally provide under a detailed technical proposal – audit and proof of manufacturing records and capability within our own country – that would be relatively straightforward and understandable. The other clarification I'm seeking is that if one takes information in the public domain and takes any (engineering) handbook, the *Scientific American,* or IEEE Journal – anything that's in the public domain – and applies straightforward engineering principles, is that under the ITAR regulations restricting data and preliminary discussion?

Mr. Femminella: Let's take them one at a time. As I mentioned the definition that we go by is spelled out right in the ITAR. It says, and I'll quote it:

> "As used in, this subchapter the term technical data means
>
> a. any unclassified information that can be used or adopted for use in the design production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction of arms, ammunitions and implements of war on the munitions list or,
>
> b. any technology which advances the state of the art or establishes a new state of the art in an area of significant military applicability in the United States, or,
>
> c. classified information."

I said earlier that it's the broadest definition that one can imagine. So, in order to transfer abroad anything that is technical data within that definition one needs a license. Promoting a sale abroad if one doesn't use technical data as defined, one is not in violation. One *can* use technical data, but yet let's spell technical with a small "t". As long as the information provided doesn't conflict with the ITAR, one can use any information needed to promote sales.

Of the three Ps that Mr. Silver discussed earlier, performance – unless it is in fact technical data as defined by the ITAR – doesn't count. It should not really be P^3 but $P^{2\cdot5}$ Sometimes performance is involved and sometimes it isn't. I don't doubt that many of you have seen the technical data in advertisements in *Aviation Week,* say, or similar publications. There are performance characteristics of aircraft spelled out in some of those advertisements. That information certainly is not technical data within the meaning of this ITAR that can be used for promoting sales. It's price and availability that we're really interested in. That's where you're really down to the nitty-gritty of signing a contract.

I don't know whether I've answered your question completely. You can use anything that will make a sale provided it's not price and availability, and that, remember, applies only to those sales that come under the rule to start with – significant combat equipment of 7 million dollars, *et cetera.*

Voice: I'm going to muddy the water. At the level I look at these things, I think the most significant change in the last year and a half, and I've been involved in these matters about six years, has been the change in the burden of proof. When one has a complex argument like this, one is trying to determine how the national interests compete. Quite frequently it's easier to answer the question as a function of the way one views the problem. I think the difficulty now is that the view that results from the President's arms control policy of last May 19th, and perhaps the Secretary of Defense Memorandum and others, is that the burden of proof is in a different perspective.

Let me see if I can explain to you what that would mean. In the past, one might say that as long as industry was acting in good faith and tried to define these things in a reasonable way and move ahead, it worked out pretty much as Mr. Femminella described. A license was approved and things went along pretty smoothly. Now, however, there has been a shift and one must prove to the government that one is not releasing certain kinds of information. If you can't present proof, the license isn't granted. I do not

believe that it is clear yet how these changes are working. It seems to me that this can be compared to one of the lumps in a python coming down stream that's planning to swallow us. I think we'll look back on these days in a couple of years and see that this burden of proof argument may have caused as much difficulty to us as just the criteria themselves. It's a very complex problem and just shifting perspectives has a tremendous amount of impact on how we deal with the problem.

I know Mr. Femminella might want to comment.

Mr. Femminella: I think the observations are absolutely true. The President's new policy has turned the conceptual approach to licensing completely around – a 180 degrees. Philosophically, a year or two ago we took a license application and said if you don't have a decent reason for turning it down, give it to them, approve it. Well, that's been reversed. The burden of proof is now with the individual that's asking for the license. If he doesn't have an excellent reason for obtaining the license, the current philosophy is to turn it down. That's the direction the policy is taking us.

THE DECISION TO RELEASE TECHNOLOGY AND HARDWARE TO FOREIGN GOVERNMENTS

Dr. Oles Lomacky
Office of the Under Secretary of Defense, R&E

The International Programs Office serves as the Department of Defense focal point for international Research and Development actions which interface with allied governments, military services and industries. It has a dual responsibility. On the one hand it is responsible for enhancing international cooperation (technology sharing) particularly with our NATO allies. On the other hand it has major responsibility in the control of the flow of advanced systems and technology either military or commercial to foreign governments.

I do not plan today to provide a formal presentation on the government-to-government exchanges. Typically these relate to the foreign military sales, coproduction, data exchange agreements, scientists exchange programs and the like. I feel that this aspect requires a separate, in-depth analysis. I plan to talk on only one aspect of the overall technology transfer problem: namely, the advisory role of the Department of Defense in commercial export licensing relating to the cases forwarded for our review from the Departments of Commerce and State.

As the result of some recent decisions with the Department of Defense, the International Programs Office will bear greater responsibilities for the processing of export cases, in addition to assuming an increased role in NATO initiatives. The manner in which the export cases are handled within DoD is a matter of considerable interest to the agencies of the government, Congress and industry. My intent is to provide you with my perceptions of some of the problems. Further I shall describe recent actions taken toward streamlining of the case review process within the context of other DoD activities in export control and technology transfer.

First, there is the basic problem relating to policy questions. In export case decisions there is a delicate balance to be achieved. Our free enterprise system, as well as the economic *need* for exports demands *least* bureaucratic interference in the conduct of international trade. Further, in the interest of NATO standardization, we want to aid and stimulate collective allied R&D efficiency. However, we must achieve this *without* either weakening the US technological/industrial base or frustrating US policy goals in arms nonproliferation. Further, we need to protect critical defense related technologies from the diffusion to potential adversaries.

Second, there is a problem of increased volume of work coupled with the demands of increased technological sophistication of export transactions. In export cases relating to dual use (commercial-military) technologies and products forwarded to the Department of Defense from the Department of Commerce, there are well over 2,000 cases per year; munitions case workload is approximately 4,000 and growing. This, of course, is in addition to the foreign military sales actions.

As you are well aware, the US government is often criticized by industry and our allies for the delay in case processing. Another source of complaint is that the division of responsibilities is perceived as being fragmented within the DoD. Finally, I am sure that you are well aware of the Defense Science Board (DSB) report (also known as the BUCY report) which criticized the government's over emphasis on control of products to the deteriment of paying adequate attention to the control of strategic technologies.

What steps has the Department of Defense taken to address these concerns? As a follow up to Secretary Brown's interim policy statement "Export control of U.S. technology" of August 26, 1977, (which, as you

probably know reflected implementation actions resulting from the "Bucy" report) Secretary Duncan on March 18, 1978, directed changes in the procedures of export case processing. While International Security Affairs (ISA) retains the responsibility for providing overall DoD positions, the Office of the Under Secretary of Defense for Research and Engineering (USDR&E) shall be responsible for providing to ISA consolidated, DoD positions on all technical, program and combat effectiveness aspects. Further, in contrast to the current practice, the military departments and other DoD components will be responsible for providing such evaluations directly to USDR&E rather than to ISA. On April 21, an implementing memo, designated the International Programs Office as the focal point within USDR&E. All supporting DoD components were provided with a detailed list of factors that must be considered in each technical review. Further, they were requested to provide a single point of contact and to coordinate the assignment of technical personnel to the export control tasks with the office of international programs. These new procedures are now being implemented.

What will be the effect of these organizational changes? Although the workload in the International Programs Office will significantly increase at first, I feel that focusing the responsibility for techno-military aspects within USDR&E, once fully implemented, will result in speedier and more competent review of all export cases. I expect also better management of this process within the services. Further, it will permit the "case processing" aspects to be tied more successfully to the DoD technology transfer initiatives. They have been underway primarily under the direction of USDR&E. These are the DSB implementation effort, NATO initiatives, Consultative Group Coordinating Committee (COCOM) and munitions list reviews. I would like to touch on some of these aspects.

First – regarding the DSB implementation and COCOM list review activity. As you may know, an intensive effort has been underway to develop a list of critical technologies and associated keystone equipment. A preliminary list of 138 critical dual-use technologies has been distributed for industry comments. Dr. Ruth M. Davis, the Deputy Under Secretary of Defense for Research and Advanced Technology, in addition to her responsibility for DoD's technical effort in the COCOM list review, is spearheading the effort – with extensive industry cooperation – not only to complete the documenation needed to establish critical technology lists, but also to devise a mechanism for maintaining their currency.

The checklist of factors for case processing requires awareness of critical technology lists. It is our intent to make *all* of the information being developed fully utilized in case processing. Similar considerations apply to the information being developed in the technical COCOM list review process. Of course, the significance of critical technologies and COCOM list review is not limited to their utility in the assessment of current export cases. We expect that such efforts will provide continuing guidance to the Department of Commerce on what cases should be sent for DoD review and reduce the number.

Second, with respect to NATO, the checklist of questions on munitions export includes the assessment of the relationship of the proposed transaction to NATO initiatives. This, of course, is directly related to our policy emphasizing the importance of technology sharing with our allies.

Finally, in regard to the changes in the munitions (ITAR) lists we intend to conduct further, in-depth analysis of the list comparable to the current COCOM list review and here again the documentation developed will be fully utilized in the assessments of cases.

In summary, I have given an indication of how the case processing system in DoD is being changed. This is done through:

- The organizational changes with greater responsibility being assigned to the USDR&E and focusing of responsibilities within supporting DoD components
- The development of improved evaluation guidelines, and
- Closer coordination between case processing, critical technologies lists, and the new policy initiatives in both export control and technology transfer to our allies. We welcome your interest and specific comments.

Questions and Answers

Question: Regarding the policy of encouraging our co-development of technology. Has the issue of third country sales and where that technology will go after it's developed been assessed? and, has there been a realistic determination of whether the Europeans will still be interested in co-development if they must be restrained on third country sales as are U.S. contractors?

Answer: Well, I said I wasn't going to talk about that problem because it requires a whole presentation. However, this is one of the perennial problems when we talk to our European allies on the third country transfers. I don't believe I can give you an across the board answer as to how this policy question has been resolved. It has been on a case by case basis.

Question from Mr. Behr: I do have a question on Foreign Military Sale procedures that perhaps you can enlighten me on – even though you said you were not going to discuss that one much. When a military service negotiates a FMS with a potential customer and the PNA is sent up from the field to the service concerned and before the PNA is released to the potential customer, is your office involved in reviewing those items which are considered negotiated for sales?

Answer: Not always. We do get involved in some of the significant items but it hasn't been a general policy to involve our office in all of these aspects. The Defense Security Assistance Agency has a responsibility for that area.

Comment by Mr. Behr: This, of course, comes back to haunt us because when the sale is completed and the guidelines are written under which the sale is to be effected and the data that is to be released for the particular sale, we are always told that DDR&E has to coordinate on the specific guidelines.

Response: That part is true. We do get involved before decision is made in the coordinating process.

Question: A question for Dr. Lomacky that relates to the CoCom list.[1] Do you feel that more and more commercial products, such as computers with some high technology in them, are going to be subject to being placed on a CoCom list?

Answer: The list of embargoed products is revised roughly every three years, and the process of revising a CoCom list is a very complex one. Each nation submits a proposal for review. Generally, the trend has been to take more and more items off the list. There is a current effort to revise the list.

You must realize that an embargo list is not absolute. Items on the list can be exported provided certain criteria are met respecting whether an exemption has been granted. Exemptions can be granted to an embargoed item on such grounds as an end use statement or perhaps some other policy considerations – economic hardship for a country if that particular export were not made, and so forth.

So that's essentially a brief capsule of what CoCom list is. Now, the question, are more computers likely to be found on the CoCom list? I don't think that's likely. I think those high performance computers with potential for military applications are likely to be retained on the list. However, the low performance computers are not likely to be placed in an embargo category.

For example, as far as the volume of export license applications that my office considers (exports to Communist-block nations), I would say 50 percent of the cases if not more deal with computers. There are all kinds of computers. The Cyber 76 that was mentioned earlier, represents the most advanced type. Incidentally, no one in the government had approved that export. I don't know how the press got that impression, but it was the almost unanimous feeling that this was a very highly strategic item and should not be exported. So, computers of that type I expect to remain on the list. Other computers of relatively marginal capability we would not think of controlling. If *we* were to control them, they could easily be purchased somewhere else, and we would not have gained a thing by denying export.

I'm afraid that was a long rambling answer to the question.

Question for Dr. Lomacky: In a CoCom case processed by the Naval Surface Weapons Center we turned the request down based on responses to your list of requested comments on and use of the equipment in question. Much later we received a call asking "Will you re-evaluate your position on this because we have pressure from a Congressman on release?" We took the stand of not re-evaluating. We said, "no; we don't believe this should be released."

Do you have any comments for the future?

Answer: I don't recall the particular case. Probably it was under the old procedures. Under new procedures you can argue with us directly now instead of a half-dozen other people.

---

[1] CoCom stands for Coordinating Committee and is comprised of the NATO nations plus Japan but minus Iceland. It's purpose is to *informally* embargo for shipment to communist bloc nations those items on which it reaches agreement regarding embargo.

INFORMATION SECURITY & THE EXPORT OF TECHNOLOGY

Charles Phipps
Assistant Vice President
Strategic Development, Texas Instruments

Introduction

The invitation to present my viewpoints on American Technology and National Security was received with not only keen interest, but also with a desire to share with you my concerns on the subject – based on experience in industry and with Government Advisory Groups.

A principal strength of U.S. weapon systems is dependent upon American technology. The advancement of technology has allowed the United States to realize a strategic advantage over the Soviet Union and other potential adversaries with a smaller number of weapons and military personnel. Today, there is serious concern that this advantage has been reduced in the last five years. During this period, there has been a concentrated effort by the Soviets to acquire Western technology, particularly in electronics and aerospace. At the same time, elements of this technology have become widely available because of the rapid industrial development of our trading partners of Western Europe and the Far East.

One of the primary objectives of any policy for American technology of military significance is to maximize the performance of U.S. weapon systems for as long as possible, as compared to weapon systems of the Soviets and other adversaries. There are two principal strategies supporting this objective. First is the continued development and application of new technology to weapon systems. This is being done, although progress often is impeded by Government regulations and bureaucratic delays. The other strategy is to control the export of technologies that are critical to U.S. weapon systems. The latter strategy is the focus of this presentation.

The Status of Export Control and Technology

There are a number of trends and events that make export control of technology a much more difficult problem today than it was five years ago. I will note only two of them:

- U.S. foreign policy toward the Soviets has emphasized an increase in commercial trade, and scientific exchanges; and,
- In some fields of militarily significant technologies, such as electronics, commercial applications are now occurring three-to-five years in advance of military applications.

For an example of the latter point, the so-called LSI integrated circuits were first applied to handheld calculators in the early 1970's. They were followed by microprocessors applied to a wide variety of consumer and industrial products in the mid-1970's. Yet, as of today, there has been only minimal application of these LSI integrated circuits to weapon systems.

We do not now have an effective export control policy that copes with the complexities of our environment and these developments. Too many of the strategic technology issues are considered in isolation from each other; and, often, they are subordinate to other policies. This situation has developed over the years because technology issues have been included as individual *elements* of disparate regulations, rather than focusing on strategic technology itself as a primary *issue* of high national security importance.

The inconsistency of Federal policies and regulations regarding export control of technology will continue to be further aggravated in the future, as new policies are developed regarding the encouragement of technology transfers to less developed countries, and, at the same time, other policies will focus on the competitiveness of American technologies versus other industrialized nations. The development of coherent policies for these overlapping areas – national security, foreign policy, and economic issues of trade – is difficult because:

- The difference between products, science, and technology is often misunderstood and,
- The fact that most American technology is privately owned is an important legal consideration in our system.

To support the concept that technology, products, and science are misunderstood and confused by most people and the lay media, consider that it is not uncommon to see the meanings of these three words used interchangeably. The specific design and manufacturing know-how required to *produce* products is really the issue and it is of major importance. That is what technology is all about. Technology is *not* products, and it is *not* science. Technology is the application of science to designing and manufacturing products and to producing services.

Technology is the specific "know-how" required to conceive & define a product that fulfills a need; then to design and manufacture it. Technology encompasses the thousands of detailed steps necessary to develop and manufacture a product – as well as the design and development of manufacturing processes and the equipment for the system.

In the aerospace and electronics industries, often the quality of one's technology is the critical element in determining a company's success. Companies that recognize its value – generally the innovators rather than imitators – the ways in which technology is used or transferred to other companies or nations are issues of greatest concern.

The transfer of technology with all its data bases should be viewed as an element of long-term strategy for corporations, and not as an opportunistic item of the immediate future. Further, those technologies that are rapidly growing – the so-called high-technology industries – should be identified and understood by corporations as, indeed, one important corporate asset.

There are various strategies that may be employed for effectively allowing the products of technology to compete in world markets – and for most industries, true competitive position is determined by their market share in world markets.

- An early strategy is to export products only, and protect technology through patent licenses – trade secrets.

- As international markets develop, usually it is necessary to have a manufacturing presence in these markets. Manufacturing technology then must be transferred. The selection of the means by which such transfer is made directly affects the control a given corporation may be able to exercise.

  - The wholly-owned subsidiary allows effective control.

  - Joint ventures with foreign manufacturers lessen the control and use of the technology transferred

  - Transfers to independent third parties. Provide little, if any, direct control.

However, in commercial practice relationships between the parties are based on experience, mutual trust, and the continuing good faith of the parties involved. So in the last case these linkages may provide *some* degree of control over the technology.

However further, the transfer of technology to a *state-controlled* enterprise is outside the framework of commercial practice and leaves the continuing relationship and control subject to political priorities. Since many portions of world markets are controlled by state-owned enterprises, corporations may need to find solutions to reaching these markets. On the other hand, we cannot afford to be foolish about it.

In each industry segment, unfortunately, some companies view their technology as another commodity for sale and others are lax in protecting their technology. In either case, the release of technology may significantly hurt not only themselves but also others in their industry in the long run; and, in some instances, our country's national security.

As opposed to technology, *science* is directed to obtaining knowledge. Scientific information and data is exchanged around the world, and in so doing it adds to man's understanding. It should continue to freely flow. Also as opposed to technology *products* are the end result. They are not technology in themselves. For instance, the impact of exporting technology is quite different from that of exporting products.

The export of products satisfies only short-term needs. It does not fulfill future requirements. However, the export of design and manufacturing know-how confers a capability on the receiving country or corporation to satisfy both present and future needs. Further, it may provide a technology base to support subsequent advances in the art, or it may be able to be diverted to uses other than originally intended (namely from commercial to military). Once a technology transfer is made, there can be no effective control of either the flow of products or future applications of the technology; once released, technology can neither be taken back nor controlled.

Those of us whose careers have been devoted to devloping technologies and applying products to new markets are concerned about this new "ball game". The transfer of technology to a third party over whom you have no control – regardless of the legalities – is irresponsible to the long-term interests of high-technology companies. The distinction drawn between design and manufacturing know-how and end-use products, is clear for most items. Commercial product sales rarely include proprietary design and manufacturing information.

There are, however, gray areas. One product category that does transfer some know-how is *manufacturing* or *process* equipment. Such equipment usually conveys only the know-how for its point-of-use in the manufacturing system. Manufacturing equipment unique to critical military products are, thus, also critical items. Another gray area is large computers. Although they are products and not technology, their application can directly advance design and manufacturing know-how. These machines are the means by which technology and know-how is extended as much as or more than they are end-use products.

Moving to the second factor – compounding the problem of export controls is the fact that virtually all American technology is the property of *private firms.* Even though Federal R&D expenditures have advanced scientific knowledge, and Federal procurements of weapon systems have advanced the translation of such knowledge to products, the underlying design and manufacturing know-how has almost always remained as a corporate property, even if there is any potential for commercial applications. Each firm develops its own specific design and manufacturing know-how although it may be similar to that of its competitors. Each advance in technology is built upon an experience base that has been accumulated over the particular corporation's entire history.

Consequently, controls on the export of technology should focus on those commercial trade mechanisms which most effectively *transfer* "know-how". The question of "reverse engineering" for products – engineering dissection and analysis so as to be able to recreate the means by which the end was achieved – is not necessarily an effective technique for transferring technology. The analyses may provide limited gain from insights perceived of the design approach, but the receiving country still is required to devote technical resources and time to developing and gaining experience in the technology and that retains advantage (albeit for a lesser time).

The principal mechanisms for the transfer of design and manufacturing know-how are those based upon special and extensive communications by the provider with the objective of teaching that know-how. Usually, such information and data are provided to the receiver so that he may achieve a stated manufacturing capability within a relatively short period of time. Thus, an effective mechanism for transferring technology to state-controlled enterprises includes control of: sales of "turnkey" factories; sales of manufacturing and technical data; license with extensive teaching; consulting agreements; and the training of technical personnel.

In addition to these formal transfer mechanisms, there are casual and clandestine transfers of technology, both of which must be guarded against. They range from peer conversations between engineers at technical or professinal gatherings, through foreign trips, and the information disclosed to casual foreign visitors (from controlled countries) on visits to plant sites, to the data included in preliminary proposals and sales briefs to controlled countries.

Toward the Future

It was with this recognition that technology is the really critical export issue, and with the identification of the principal transfer mechanisms as just noted, that a group of senior industrial and government participants in a task force for the Defense Science Board underscored these recommendations:

- That the emphasis on export controls should be shifted from products to critical technologies. This requires a clearer definition of critical technologies than has existed.

- That these critical technologies must be defined by the Defense Department, based upon:

  - Their use in the more significant weapon systems of the present or future.

  - Whether they are principal technology drivers: along with their past rate of advance, and probable future rate of advance.

  - Their current practice in controlled countries and,

  - Their commercial availability among Western nations.

- The strategies for implementing control of critical technologies should recognize:

  - That the chief criterion for assessing the impact of a technology transfer is not whether it is obsolete by U.S. standards, but rather the degree to which it would advance an adversary's capabilities;

- That each technology is time-dependent in its singular value to U.S. weapon systems, and, therefore, the criticality of a given technology needs to be periodically reviewed; and,

- That critical products that do remain under control should be controlled on the basis of their intrinsic utility, and not on the basis of commercial specifications, end-use statements, or safeguards.

Such arguments ignore the negative impact of present practice. Ambiguities, long delays, and excessive focus on a product's commercial specifications, result in the process being held in low esteem by segments of industry and some of our allies. A clear definition of critical technologies is necessary to win support from our allies. Turning to the neutral nations, if we cannot control reexportation of critical technologies from them, there should be serious question as to whether they should be transferred to them.

As to the last objection, I believe just because we cannot prove quantitatively whether export controls have helped or hindered the Soviet military effort, there is no reason to "throw the baby out with the bath water." Not all logical deductions can be quantified, and when attempted, the available data are often subjective or poorly supported empirically. However, a lack of quantiative measures then places greater reliance on the judgment of senior policy makers for definition and implementation.

Improvement in the effectiveness of these controls can only be attained by the U.S. clearly defining its objectives, implementing them with consistency, and communicating this information to all interested parties. The issue is effectiveness of existing control mechanisms, and not one or more or fewer laws or regulations. In other words, an intelligent approach must be taken toward the control of technology and critical products of military significance. If this can be achieved, *then* the U.S. can gain improved support from industry, its allies, and the enforcement agencies.

Concluding Observations

The challenge is to effectively implement a policy that will allow the U.S. the best means of achieving two conflicting goals:

- Enhancing East-West trade, particularly in "high technology" products and science contracts

While at the same time

- Relying on technology to provide a qualitative advantage for U.S. military systems.

Given the complexity of today's weapons systems and the rapid dissemination of high technology goods and services through the world through commerce our national security will be placed in jeopardy unless we can effectively delay the acquisition of critical technologies and key products by the Soviets and her allies. The overwhelming consideration in controlling technology transfers must be U.S. national security and the military balance of NATO versus the Warsaw Pact.

In addition to the commercial trade mechanisms for transferring technology, similar controls for critical technologies must also be applied to: weapon sales, government-to-government science and technology exchanges, and other non-commercial transfer mechanisms.

The control of critical technologies does not need to be absolute in order to be effective. Their objective is to delay their rapid acquisition by the Soviets and other controlled countries. Even though U.S. export controls and those of its allies have been less effective in the past five years than in prior decades, they still provide some measurable lead time in the practice of these critical technologies by the U.S. and its allies. Various research institutions, industry committees, and the intelligence community continue to estimate that lead times are 3 to 10 years for selected technologies.

As is often the case when major policy changes are proposed, objections arise either because there is uncertainty about their implementation, or because of ignorance and distortion of the need for the policy. From industry's viewpoint, a negative reaction to changes is based on past experiences, in which Federal Government policy changes often resulted in a more negative than positive impact on industrial and commercial trade practices.

In this case, uncertainty is increased because specific definitions for critical technologies are lacking. Uncertainty will continue until critical technologies are defined and put into practice by DoD. Unfortunately, DoD has given minimal support to the administration of export controls over the past five years and other Government departments have serious doubts about DoD's ability to carry foward and implement such a policy.

Other objections by individuals in the Federal Government to change in emphasis of export control policy from products to critical technologies that have been noted in the past year are:

- The present controls have been effective in controlling East-West trade, and only fine tuning is needed, rather than a major change.
- The principal problem in commercial trade is really West to West to East flow. However, it is not practical for the U.S. to enforce controls on reexportation of technology from either its allies or neutral nations and,
- There is no data base to support the control of critical technologies, and since it cannot be quantified and measured, there is no basis for formulating policy.

Such a position is consistent with the national policies and needs of the U.S. However, true only if the bureaucrats curb their appetite for controls, and *really* limit them to truly critical technologies of commercial trade. If not, the morass of red tape controls will force on this country the undersirable alternative of abandoning all controls on commercial trade. There are indications that the Congress – under justifiable pressures from their respective individual constituents – is moving in such a direction; at least in regard to national security issues.

Philosophically, the elements are enjoined in two divergent viewpoints. Federal policy change and its implementation is approached as a *long-term change* by individuals in the Executive Branch. Industry, on the other hand, is faced with *near-term decision* and action regarding commercial trade and national security issues. The immediate task requires a realistic identification and definition of critical technologies, and the implementation of strategies for effectively controlling them by the U.S. and its allies. For the long term, the protection of American technology as a vital resource of this country, is dependent upon an increased awareness of its value by policy makers both in the private and public sectors.

When the private sector recognizes that the only adequate payment for "high" technology is "market share" derived from the long-term sale of products in world markets and that technology is basic to long-term strategies of the Corporation for its survival, then such technology will be effectively protected by its owners.

Then, in the public sector, the development of specific goals and policies for the more critical segments of American technology is mandatory. These policies must *not* be allowed to become a rallying point for a whole new set of laws and regulations resulting only in more Federal interference. Instead, such a policy should place in perspective the vital contribution of technology to the security and economic development of the U.S., and recognize that *technology* is most effectively advanced through private ownership.

NATIONAL SECRETS & THE MEDIA

Benjamin F. Schemmer
Editor, Armed Forces Journal

Last night at your President's reception, they introduced me to three more guys who have investigated and bugged me in the short ten and a half years that I've been a journalist.

But I couldn't find the ones I'd really like to meet – the team that broke into my Georgetown home three weeks ago, left the back door open, snuffed out two cigarette butts in the potted plant next to my bed, and left the phone off the hook. My friends in the Pentagon insist it wasn't their bug – probably Israeli or East Germany, they suggested. But I know an Israeli bug when I see one – they're not as smooth.

In 1973, I spent three weeks in Israel as a guest of their defense and foreign ministries. I wrote my wife every day. Toward the end of my stay, my wife called and said, "Your letters are being opened." My hosts denied it. When I got home, my wife thanked me for corresponding so faithfully. As we leafed through and talked about all the letters I'd written, I asked her, "Why on earth did you say our mail was being opened? "These look fine." "They are," she said, "but look at the holes: you've never clipped two-page letters together with a *straight pin* before." Still, I thought she must be mistaken. But I got home early in June, and I knew something was wrong when my last letter to her arrived in mid-August – by the time I'd left Israel, I was really lonesome, and my letters must have shown it. Pinned to the upper left corner of the last one was a note scrawled in Hebrew on what looked like a torn corner of toilet paper. I took it to a friend at the Israeli Embassy in Washington and asked him to translate it: "What's it say?" "That's Hebrew for your equivalent of, how do you say, 'Must be a Lucky Devil,'" he told me.

The Israelis, you know, have a clever way of handling press leaks. Censorship is very strict. When they want something to get in the public domain, they leak it to a foreign journalist abroad. Once it's printed

overseas, Israeli papers are free to print it without inhibition. It's a system that has greatly improved our Mid-East reporting.

But my problems with the Fuzz are nothing like the President's. One of his key appointees, who refuses to work that late at the office, had an 800-lb. safe put in at home just a few months ago – early this year. The only problem was that after it was installed, some of the security types screwed up the combination – and couldn't get it unlocked for 3 weeks. I was told I could *share* that story with you, but not *print* it.

Just a few weeks earlier, something similar happend to a friend of mine, suspected – incorrectly – of leaking some highly classified information to the *Journal*. The Fuzz busted into his vault; not one of them, incidentally, was cleared for what was in it. They changed the combination – and lost it! "Doc" Cooke will deny that ever happened – but Doc, there are some things the Fuzz won't tell even you!

I know how concerned you are about leaks to the press, and I share your interest in those leaks. In my case, I'm all for them.

In February, we all read a rash of new stories about Defense Secretary Harold Brown's "Draft Consolidated Guidance" to the Services for preparing their FY1980 defense budgets. Although the document was secret, many reporters – including our own – quoted verbatim from it. I know of four newspapers or magazines which had virtually complete copies of that document. In a two-week period, *we* obtained three of them: two of them came blind, by mail, in plain envelopes addressed to us, typewritten, with typewritten return addresses – ours. (That was some of the least interesting mail we get, incidentally.)

Members of the Senate Armed Services Committee expressed great concern over the leak of that document. (I know – two Senatorial offices called us asking if they could borrow a copy!) What's interesting to me is *not* the leak – I take the leak for granted; I *expect* leaks – but what did *not* get printed.

That document, classified only Secret, contained, among other things:

- A breakdown of the National Security Agency's budget, by year, FY 1979 through FY 1984;
- A bean-count, by type, of theater nuclear weapons deployed in Europe.

There was no designation on it noting information "restricted" under the Atomic Energy Act; no prohibition, caveat, warning, or designation about Executive Order limitations on intelligence agency budgets.

I'm sure I'm not the only reporter who saw those data, or recognized the potential news value of them. Yet not a word of them got printed.

That raises two questions:

- How *bad do* leaks hurt?
- *Why* do leaks occur?

The first question is easy to answer:

I defy anyone in this room to name one instance in which a newsleak in the American press during this century has ever caused harm to our national security. In the Civil War it was different. The *New York Tribune,* for instance, printed a detailed account of Sherman's plan for his march to the sea 2 weeks before he launched it – apparently, the War Department didn't subscribe to the *Trib,* or found the alleged plan so unbelieveable that it didn't bother informing Sherman of the compromise, because he executed it as advertised.

I know of no responsible official, active or retired, who can name an incident in which a press leak has hurt this country, and I've asked many of them about the issue. I don't call Philip Agee's CIA book, incidentally, a "press leak" – he's not a member of the press, and I don't know of any editor who would hire him. Agee *did* hurt, incidentally.

Then, to the second question; Why do press leaks occur? *First,* they occur because documents are poorly, carelessly, cavalierly classified. Harold Brown's "Draft Consolidated Guidance" is one recent, and telling, example. Unless you people have changed classification procedures in ways I haven't seen in my 10 years out of the Pentagon, it should have had some 5 different classification stamps on it in one place or another.

Second, they occur because documents are overly-classified. A good example is budget-sensitive data that is too often classified Secret – like a memorandum we recently printed in full from the Under Secretary of the Navy to the Secretary of Defense detailing his Department's objections to a proposed FY 1979 budget decision on naval aviation programs. There was *nothing* in that paper that qualified for any Top Secret, Secret, or even Confidential classification under

the guidelines laid down, for instance, by the new Executive Order on National Security Information.

The document was classified only because it was *budget* sensitive. But that won't hack it, and responsible people who take issue with sensitive budget decisions *know* that excuse won't cut it; the practice of so classifying documents needs to be eliminated. All it does is make a mockery of the real purposes of classification and emasculate the import of classifications on documents that properly should be. I printed the document in full after a few sentences from it leaked in the *New York Times,* and the Secretary of the Navy told the Senate the leak was "unfortunate" because it quoted the memorandum "out of context." That was so much bilge – the memorandum had been quoted precisely in context: the "system," however, found embarrassing the disagreement it revealed between one Presidential appointee and another.

A *third* reason documents leak is that the people who classified them want them out in the open. After all, you guys have made it easier to leak a Secret than to declassify one. And I want to tell you, *this* ship of state leaks from the *bridge.* If you're checking *me* out for the source of some of our stories, don't bother ferreting out the basement or bowels of the Pentagon – check the E-Ring. Don't worry about some obscure government bureaucrat or field grade military officer. Complain to the White House or some very senior NSC officials in the Executive Office Building (EOB).

In fact, the times I've been chewed out worst about a leak happened when I *didn't* print one. When Henry Kissinger was the President's advisor on National Security Affairs, for instance, an unnamed senior NSC official invited me to lunch one day, and in strict confidence – ("this is not for publication, you understand") – told me of four major new Soviet ICBM programs that were jeopardizing our SALT negotiations.

At that time, the *Journal* was a weekly. Ten days later, he called me to an EOB office and literally *shrieked* at me. Why hadn't I printed that story? Couldn't I tell an exclusive when I saw one? I'd blown a great way to get a subtle message to Moscow. The next morning, I read most of the "Secret" I had so carefully "protected" in the *New York Times.*

A year or so later, the same official invited me to lunch once again – at the White House mess. He needed help. We had just raided Son Tay prison in North Vietnam – the raid succeeded, but the camp was empty. The Pentagon would announce it all within hours. But, he needed help. His office had an odd report that the raiders had not really returned empty-handed. They had kidnapped a baby North Vietnamese water buffalo.

His question: Could I help *find* it!

I was somewhat dumbstruck. Why me? Why couldn't the White House, with all its resources, find it?

He told me, "You don't understand. We invaded North Vietnam – and all we have to show for it is a god-damned baby water buffalo. We found traces of water buffalo dung beneath the helicopter floor boards. And we think the raiders are hiding it to keep as a mascot. We'll be the laughing stock of the world. But, if *we* investigate it, word is *bound* to get out. But maybe you can quietly inquire – you know a lot of people involved – since no one attaches any significance to stray voltage from a journalist, but stray voltage from here is something else." Within three or four days, I telephoned back. The official was out, so I left this cryptic message: "Don't worry about illegitimate baby. You're not pregnant." Within hours, I got called back to the White House. How did I *know?* Could I really be *sure?* And then the official insisted I tell him, by name, rank and serial number, whom I had checked with. I left his office in something of a huff – after telling him if he asked me one more such question, the cover of my next issue would have one simple, big headline:

"VIETNAM WAR AT A STANDSTILL WHILE NSC HUNTS FOR STOWAWAY CARABAO"

I did not speak to that individual privately for almost four more years; after I'd asked him to review, off-the-record, a draft of my book, *THE RAID.* He had read, in the book's epilogue, a truncated account of the story I just told you.

He had just one question – four and a half years *after* the Son Tay raid: How could I be so *sure* that our Special Forces troops *weren't* harboring an alien baby water buffalo?

But let's take a more recent example. In our May issue, there's a story that the U.S. may deploy close to 11,000 cruise missiles. I put that story together from a variety of sources, mostly Secret documents leaked to us over the past 3-1/2 months.

Concerned over its SALT – and other – implications, I informally sailed it by several senior admistration officials. They all asked, "Hmmm, How did you arrive at the number '11,000'?" I told them. The common reaction was, "Gee, I never really added them up that way. That's a good story." Still concerned about the leak, I showed it, finally, to a "senior official" of the NSC staff. He read it carefully, and then asked: "When will this issue be off the press?" I told him the date. And he asked me very simply, "Is there any way you can plant this with a wire service a day or two ahead of time?"

So – Gentlemen, Ladies – my message is simple: You have your job to do, investigating my leaks; and I have mine to do, printing them. But the next time you bug my house, put your cigarette butts out in an ash tray – my favorite potted palm died last week!

Ed. Note: Unfortunately, the recording system did not pick up questions in this question & answer period. Although Mr. Schemmer's answers were transcribed it was not possible to reconstruct what the question or observation was. Where reasonable, it was done (based on "reverse engineering" from the answer). One question obviously related to the "Glomar Explorer" case to which there was a long response from Mr. Schemmer part of which was a rather humorously presented anecdote that deserves inclusion.

I specifically looked into [the effects of the Glomar Explorer release]. I've been very close to some of the people who broke the story. One of my best friends had a 19 inch antenna put underneath his coffee table because of part of the Glomar story that he broke in *Time Magazine.* I was appalled that you guys still had such long antennas in this age of technology . . . The trouble with that antenna was – otherwise it never would have been discovered – that while they were very careful when they put it underneath the coffee table to use a very special varnish that matched in color the varnish underneath his coffee table, they didn't quite chemically test it correctly and the epoxy reacted negatively with the varnish and the antenna started drooping down, And, you know, this long thing underneath this coffee table became kind of obvious when he was crawling around the floor looking for his contact lenses or something like that.

Incidentally, one of the interesting things about that antenna is when it was turned over to the FBI to find out why somebody was back into domestic surveillance, especially on newsman, they took many, many photos of it, but forgot to put a dime or a ruler in the photo. So, there are all of these photos in the file of a 19-inch antenna that could be 1 micromillimeter long."

After that ancedote, Mr. Schemmer asked if Mr. Van Cook would care to "defend" this draft Executive Order under discussion. Mr. Van Cook touched on some of the rational concerning access to lists of Special Compartmented Programs by the Director ISOO and on the legal implications of the "Balancing Test" as the reason that it was included only in the declassification phase of the program.

Questions and Answers

Comment: Your observation that there had been no "leaks" in this century that had damaged national security needs comment. There are and have been many leaks that have caused damage to the national security and no, I can't give you the details. But, I can tell you this. You and all of us are going to be paying for these things. I think one of the dangers to our national security that we in this Society have to reckon with is editors, writers, and people in fields like that, who determine that they have the knowledge of what is and what is not national security information. In honesty, they are not qualified to do that. They may be good writers, or editors, but not authorities on what is and is not national security.

Response: That point is very well taken and I agree with you totally. I'm not an authority, which is why I care enough to steal the very best and do what many journalists do – it's not unique to me. When I've got a story – cruise missiles or whatever – that gives me gas pains, I *do* check it out with people. You know, there is an unfortunate gap in this country. We don't have an official secrets act. I proposed in 1969 that we have one. I proposed that in an editorial which went over like a lead balloon. There *is* an unfortunate gap. There is no formal mechanism by which a journalist in this country can take a manuscript to the Department of Defense or NSA or CIA and say, "Hey, I'm concerned about this. Could I have it veted?" I tried that with by book on the Sontay Raid, which the *Washington Post,* I said, believed contained more intelligence secrets in one set of hard covers than had been printed in any newspaper in this country in a decade and that observation was completely unfounded. The manuscript was thoroughly veted but informally.

If leaks have occurred in the press that have done damage to our national security, I would submit to you that neither the House nor the Senate Intelligence Oversight Committees could yet name one. If such do exist, your agencies and your people in this Society

could make your jobs easier by giving them some examples. I'm not suggesting that either I or the *New York Times* print them, but those are the poeple who are trying to help you and *they* don't know of any. I'm not suggesting that Frank Church is the world's best authority on this sort of thing, but there are responsible people on those committees who can help you. But you're right, I'm not qualified.

Question: Ed. Note: A question was asked but was inaudible. It related apparently to the usefulness of the Freedom of Information Act as viewed by the press. The answer follows.

Answer: You know, as a newsman, I don't find the FOIA very helpful because I don't really need it that much. I've used it a few times. It's easier to steal a document than to request one. I think it's well administered and DoD does a splendid job of working under it. I think your agency does. My big concern with the Freedom of Information Act is that it has opened a Pandora's Box. There are a lot of foreign counsellors and persons from foreign embassies in this country, a lot of them; counsellors, commercial counsellors, press counsellors, economic counsellors, quasi-political counsellors. There are a lot of attaches who, under the Freedom of Information Act, are asking for their files from DoD, the Pentagon and "The Agency," and they're getting them. It makes it a little harder to do work. So, I don't like the Freedom of Information Act because it doesn't close any doors and some should be closed.

THE PRACTICAL OBJECTIVE

Arthur F. Van Cook
Director, Information Security
Department of Defense

I would like to precede my comments on the Executive Order with some on change within DoD affecting foreign disclosure. I believe they may be of interest at this time since there have been presentations on the international scene and more are scheduled.

In January 1978 the function and the responsibility and authority for foreign disclosure matters were transferred from the Office of the Assistant Secretary of Defense, International Security Affairs to the Office of the Assistant Secretary, Comptroller. Those functions, responsibilities and authorities now rest in my office. These include all foreign disclosure matters, national disclosure policy and the management and operation of the foreign disclosure automated data system. I am designated Chairman of the National Disclosure Policy Committee and I find that to be a very challenging undertaking.

You may find it of interest to note that the security surveys required by the National Disclosure Policy Committee to be conducted in countries where we export our classified information had not been performed in Europe, for example, since the 1967-69 timeframe. Since I've assumed the responsibilities we have had two teams in Europe, and two weeks from now they will have completed the NDPC security surveys in five countries. They include the United Kingdom, Belgium, the Federal Republic of Germany, Italy and Norway. Surveys in Japan, Korea and the Middle East are scheduled for summer and fall.

Turning now to our particular topic, I thought it would be interesting to see what has been said before about downgrading and declassification, and what realistic objectives in a downgrading-declassification program might be. I found in an earlier NCMS Journal that the designers of the automatic downgrading and declassification system expected that effective implementation would accomplish these things, it:

- Would preserve the effectiveness and integrity of the classification system;
- Would eliminate the classification of information that no longer required protection, thus reducing the accumulation of classified material;
- Would make more information on government activities available to the public; and,
- Would reduce costs incurred in storage and handling of classified information.

Now, subsequently to the time those objectives were stated, studies were conducted, and the studies concluded that the implementation of the automatic downgrading and declassification system was not attaining fully the objectives for which it was designed.

It was found, for example, that declassification of Group IV material after 12 years as we knew it under EO 10501, or the present, 10, 8 or 6 years, under EO 11642, is not resulting in a reduction of storage and handling costs; nor does such action contribute materially to informing the public on government activities. At most, declassification after 12 years, or 10, 8 or 6 makes certain information and material more readily accessible to historical researchers. I'm

quoting from the NCMS Journal. The writer continues to say: "it is my considered opinion that continued protection of technical information, much of it obsolete, for these extended periods results in an unnecessary expense to defense and industry and is not conducive to preserving the integrity and effectiveness of the classification system."

The article goes on to say that costs associated with the handling of classified material in transit and with top secret inventories can be reduced substantially when downgrading, declassification, destruction, and retirement actions are accomplished within a reasonable time after the date of origin.

The writer says also, "I believe that downgrading and declassification objectives should be those that can be achieved realistically. "I believe," says he, "that effective implementation of a downgrading and declassification program in the Department of Defense and defense industry should accomplish these things –

- Preserve the effectiveness and integrity of the classification system;
- Reduce classified inventories in the DoD, and defense industry to the minimum consistent with operational requirements;
- Reduce costs associated with the handling of classified material in transit and with the conduct of top secret inventory."

Other objectives, such as those mentioned earlier in connection with the automatic system – to make more information available to the public and to reduce costs incurred by defense and industry in the storage of calssified material – were not, in the writer's opinion, realistically related to a downgrading and declassification program.

Speaking to the making of more information available to the public, *downgrading* certainly would not achieve such a goal and *declassification* outside a meaningful timeframe does not contribute materially to the attainment of such an objective. Declassification does make information more readily accessible to the public but the Freedom of Information Act (FOIA) does not carry with it automatic public release. The writer was alluding to the fact that declassification removes only one bar to public release. Under the FOIA there are eight other exemptions that need to be considered after declassification comes about.

Further, downgrading and declassification actions appear to have little or no effect in reducing storage costs. A document once classified and stored remains a document stored after the classification is lowered or removed. Classified and unclassified documents are commonly filed within the DoD and industry by subject. Those once classified and filed usually are not removed from one storage container to another offering a lesser degree of physical security protection when the classification is lowered or eliminated.

Downgrading appears to have no effect on reducing the overall classified inventory. It changes the inventories at different levels, but the overall classified inventory remains unchanged. At most, it can be said that early downgrading may save dollars while making the downgraded information more readily accessible to those having a need for it. I should note that the article I was quoting was my own and appeared in the National Classification Management Society Journal in 1967; nothing has changed with respect to downgrading and declassification since that time. I think the objectives as I've outlined them are, in fact, realistic objectives and can be achieved; but with respect to more openness, downgrading just doesn't do it.

The new Order merely says that downgrading shall come about when it serves a useful purpose. There's nothing in the new system about *automatic* downgrading. We will have to determine when downgrading serves a useful purpose when preparing implementing instruction for the new order and guides prepared in the Department of Defense will identify information eligible for downgrading and when it will be eligible.

We have covered the changed declassification policy of the new Executive Order. It is hoped that the time period for classification will be shortened. Remember that declassification under the new concept will be based on the expectation of a loss of sensitivity of the information with the passage of time and will not be related to the original level of sensitivity as the GDS system under EO 11652 is. Actions we take in downgrading and declassification are philosophically basic to the classification system; they preserve its integrity and serve to achieve that goal.

There are costs that can be reduced. However, it's very difficult to establish dollar values; how much does one save; how much cost does one avoid by downgrading and declassification? This is true despite the fact that we have been working toward such a goal for many years and this despite the fact of many active

declassification programs and the wealth of information that the National Archives and Record Service has made available.

In closing, I agree fully with Mr. Buckland whose remarks follow, that regarding the 20 year review, if people and resources are not made available to do the declassification review, it's not going to work. This point has been made with the drafters of the new Executive Order from the beginning.

DOWNGRADING AND DECLASSIFICATION

James A. Buckland
Senior Security Specialist
Martin Marietta, Orlando Division

One always supposes that anything will work given sufficient resources – time, money, people, and training. Mr. Van Cook has presented an outline of the practical objectives of the revised downgrading and declassification program as set forth in the Executive Order, along with the basic philosophies underlying the program. In principle, I agree. But then, I also agreed with the General Declassification System; and before that with the Atuomatic Time-phased Downgrading and Declassification system; and before *that* I did what I was told.

For all of the prior systems for downgrading and declassification, if we ask, "Did it work?" the answer apparently must be "no" because the systems have been discarded. However, it would be unfair not to say that each system was some improvement over the one it replaced.

Why didn't the old systems work? From my viewpoint in industry I believe that the failures in the systems were caused by:

- The fact that the systems were based on sensitivity/time rather than on sensitivity/perishability.
- The lack of prompt, current, detailed, security classification guidance, and delayed or inadequate guidance reviews.
- The perpetuation, and sometimes initiation, of unrealistic, downgrading and declassification requirements caused by our procedures for marking derivative information.

It is interesting to note as well that shortly after EO 11652 was issued, budgets were cut in government and industry alike. As usual, overhead budgets took the worst beating. In general, where security staffs needed support – in order to implement and follow through on the provisions of EO 11652 – they were reduced in strength.

Will the new downgrading and declassification system work? I believe that the answer is "Yes", If the new plan is implemented realistically and supported with adequate resources – time, money, people, and training. I *believe*, on the other hand, that the answer will be "No", if we continue to operate in the same general manner that we are operating today and have operated previously.

In August 1977, the Society, in its recommendations to the *Ad Hoc* Committee responsible for drafing the new Executive Order stated

> "Departments having original classification authority must issue classification guides. Such guides will be prepared at the earliest practicable time, but in any event prior to initial funding of a classified program, project, or plan."

Guides were to be reviewed at least every two years. Guides were to identify what information is classified, at what level and for how long. We placed these requirements in the section authorizing Original Classification. Words to this effect are still in the new Executive Order, but they are in the section concerning implementation and review, and only indicate that "the preparation and promulgation of security classification guidance will be ensured".

Classification guides probably are the single most important items required to insure the success or failure of the downgrading and declassification system. Agencies and Departments charged with the responsibility for preparing classification guides must be funded and staffed to insure that the following will be accomplished:

- Prepare guides prior to the initial funding or implementation of a plan, program or project. If one knows enough about the subject to ask for money it seems safe to assume that one knows enough to prepare classification guidance on the subject.

- Insure maximum dissemination of the guides and/or maximum availability of the guides. Maintain the DoD Index of Guides and require all other agencies to maintain a central index of guides. Have all guides available through a central source with by direct access for those who need them. It should be noted that unless the guides are classified they are subject to FOIA requests.

- Review guides as frequently as necessary to insure that the need for classification still exists, but not less than once every two years.

- *DO NOT* upgrade or extend dates determined for downgrading or declassification. It is virtually impossible to notify all holders of the information.

- Coordinate all guides, from all agencies at a central point, possibly the ISOO. Consistency and compatibility is mandatory. Such is not true today and never has been.

- Provide a system where all organizations and/or individuals may submit recommended changes directly to the original classifier, and set a time limit for responses.

Probably the greatest cause of unnecessary classification, over classification, and extended classification is the derivative application of classifications from source or reference material. This could be called the "perpetuation of the species." Paragraph classifications have eliminated much of this problem as far as classification is concerned. However, historically, we apply the most restrictive of the declassification markings to the entire new item being generated. For example, in a specific contract all information is subject to the GDS except that which pertains to countermeasures which is XGDS(3). In a contractually required document we must discuss nuclear vulnerability which involves SECRET RESTRICTED DATA. We consider also TEMPEST problems which are COMSEC data. In discussing systems threats we extracted data from a foreign originated document. The most restrictive marking is RESTRICTED DATA. Then comes foreign originated information, XGDS(1), 30 years; followed by countermeasures, XGDS(3), 15-30 years; followed by the vast portion of the document which is GDS. Once the most restrictive downgrading is applied to the document, the rest of the downgrading instructions for the balance of the information are lost. There appear to be several solutions to this problem:

- Eliminate derivative markings and require every document (each item of information) to be classified in accordance with the classification guide for that information.

- Apply the most restrictive markings to the overall item and then require individual downgrading/declassification markings for items of information within the item much the same as paragraph marking.

- Use multiple downgrading statements for specifically identified information groups of data.

Admittedly, these solutions appear to present a "Catch 22" choice, but they will aid in making the downgrading and declassification system work.

With the advent of the new Executive Order, we have been hearing such about "Systematic Review". Let me quote from the most recent information available to me, the December 1977 draft of the EO "Classified information constituting *permanently valuable records of the Government* as defined by *44 U.S.C. 2103* shall be reviewed for declassification as it becomes 20 years old". Additionally, "Agency heads shall . . . after consultation with the Archivist . . . and review by the ISOO issue guidelines for systematic review covering 20 year old classified information . . .". Please note that these guidelines are for 20 year old material which is a permanently valuable record of the Government. It must be assumed that industry and the academic institutions do not have these types of records. It must also be assumed that most of this information will be in Government records centers or holding areas. Therefore, these guidelines will only have a collateral or spinoff effect on vast volumes of classified information. It appears mandatory that the Systematic Review Guidelines be matched at all times to current classification guides to insure compatibility. It also appears mandatory that these guidelines be compared to each other for compatibility and that they must be constantly updated to meet changing situations.

The new Order appears to set forth the appropriate requirements for a successful downgrading and declassification program. However, these requirements must be properly implemented. All actions concerning classifications and declassifications must be coordinated thoroughly whenever these actions affect, in any manner, users outside the originator's activity. Last, but most important of all, concerned organizations must be funded and staffed to meet the demands of the program.

Questions and Answers

Colloquy Mr. Van Cook: One of the things Mr. Buckland mentioned was the earlier recommendation that we insure maximum availability of the guides and maintain a DoD index. I think that the DoD Index of guides has been well received. There are over 800 security classification guides in the index now. We have also, as can be noted from the foreword, made guides available from a central point; the Defense Documentation Center (DDC). So, any DDC user can go directly to the DDC and get a security classification guide. I hope that will work.

Jim, you also made the point that all guides from all agencies must be coordinated at a central office. I hope you meant to say there that possibly there would be a coordinated listing at some central point.

Mr. Buckland: The reason for the point on coordination at a central office is to eliminate existing conflicts between and among guides. Unfortunately all the examples are classified. However, on *an* existing item with which we deal for one service it's classified, and when I pick up the other service's "book" the identical information pertaining to the identical piece of equipment is unclassified. This phenomenon is not uncommon.

You made the point, Art, that any user of DDC can go directly to request available guides. When asking our technical library about requesting guides, they said, "Fine, but send it through your contracting officer." I don't feel it should have to be sent through a contracting officer. It may be an independent research and development item of potential military application. I need to be able to go to DDC directly. Martin Marietta is registered with a field of interest and I should get the guide. I don't want to go through the contracting officer. I would like a direct route to get the guides.

Mr. Van Cook: Bob (Green, DLA) can you comment on that? To obtain a security classification guide that is available at the DDC, is there a need to go through a contracting officer for that purpose if a contractor is a registered user of the DDC?

Ed. Note: The response of Mr. Green was inaudible but the thrust seemed to suggest that the contracting officer route was required for verification of field of interest or need to know.

Mr. Buckland: Well, then my question is, "why do I need to establish a need-to-know on *that* guide in the sense that you're describing when my next door neighbor can write into the right place and pick it up under the Freedom of Information Act just because he's curious?" And, I believe I'm right that classification guides, unless classified, are available under the FOIA. If so, anybody can get one except industry with a need but burdened by the contracting office request route that you're describing. This is the problem I was hitting particularly, Art I *know* where the guides are. It was the fact of availability *and* direct access.

Question: I would like to ask of Mr. Van Cook. We have approximately 300 to 500 DD254's a year. Why is it that the User Agency consistently puts on 20 or 30 year declassification and sometimes this is applied to third or fourth generation equipment or hardware information? I think that somebody should instruct the procurement agencies on how they should downgrade or declassify.

Answer: I assume we're talking about some item of information in the DD Form 254 which qualifies for exemption from the general declassification schedule. It's 30 years under the present rules, 20 years under the new rules. I remind that in the case of scientific and technical information DoD, at least, talks about a 15 year rule. Without details I can't answer the question. I know that we've talked about this problem before and we will continue to talk about it. We encourage recipients of classification guides including recipients of DD Forms 254 to challenge classification. We've gone over that ground many, many, times. If a problem doesn't come to *somebody's* attention and you simply accept what you receive, would anyone feel there was a problem that needed solving?

It seems to me that if one receives a DD Form 254 which one must use and one believes that the duration of classification is too long, say so. Not only have Mr. Liebling and I urged such action but also others in the entire DoD structure – challenge what you think is not right.

Challenges are the only solution to the problem. For example, we appear to have a problem in DoD of over-use of exemption category 3 specifically, and we know that. But, if somebody doesn't challenge it, there's not much we can do about it – I never see the DD254.

Comment: An example can be cited. There was some equipment due to be declassified in 1981 when suddenly it was changed to declassification 2007. We pursued that problem through to the top Army Command; they did nothing about it. They didn't even respond to our letter giving a reason, and the equipment is fifth generation, designed in 1961.

So, the reason we repeatedly bring attention to this point is that despite your comments, and taking advantage of the offer still leaves a continuing problem.

Response by Mr. Van Cook: I recognize the problem. I guess we keep falling back to saying it's a matter of communication and education. I know the DLA's Industrial Security people are trying to do that. *We're* trying to do it and we still come up with the problems that you're outlining here. One hopes that the new Executive Order will help us along those lines, and that we will get a better review. One hopes also that the DD254 will do a better job for us in getting classification guidance to contracting people, but it's something that we have to continually work on and strive toward. I'm sure Colonel Pruett would join me in saying that if one goes the route, and doesn't receive a satisfactory response when there seems to be a ridiculous situation, both of us want to know about it, and I think we can move them.

Mr. Buckland: A comment on two problems that are inherent in the discussion. One is the need for a review of the guides at least once every two years. I used the example of a 1973 guidance being used in 1978 – not in your index anywhere because it was never formalized as a guide, and was not updated or replaced. The two year review should help this case.

The other is to provide a means by which one can go directly to the original classifier, with a time limit set for responses. As commented: "we wrote, we got no response". I'm recommending that such circumstance be covered in the implementing directive. That possibly would help reduce that particular problem. I think that what I set forth is basically in agreement with the points you made. However, I believe that if written into the implementing directive it would have "teeth".

Question: We have talked about the 30-year rule now being changed to a 20-year rule. Would you comment about the 15-year rule, for scientific technical information, and how this will be handled under the new Executive Order?

Mr. Van Cook: The Navy started putting a 15-year rule on scientific and technical information and it was extended to the Department of Defense. Our regulations provide that if you're dealing with scientific and technical information it is reasonable to believe that obsolescence occurs rather early. When one exempts information on that basis one should provide that such information be declassified within the 15-year period.

The DoD has been and is acting, of course, within the parameters of the existing Executive Order or its implementing National Security Council directive; it is bringing about earlier declassification. We elected to go that route with that kind of information.

I think we'll continue to go that route under the new Executive Order and it's certainly permissive for us to do it to bring about earlier declassification and where we can do it, we will.

CONTRACTING OFFICER'S PROBLEMS

Edwin W. Yokum
Space and Missile Systems Organization

Summary of Presentation

Mr. Yokum began his presentation by noting that some ten years ago that he had discussed the need to involve User Agencies – the ones that actually contract for the researches as well as those who determine requirements (*e.g.*, HQ, USAF, CNO C/S Army do not contract; they have a material/research agency under their jurisdiction contract while they determine amounts of money, thrust, performance, and requirements).

He noted that he enjoyed "being in the trenches" of the determination, applications, and questions from contractors. In the case of SAMSO he commented that their mission was to "plan, develop, acquire, launch, and *operate* . . ." observing that not all User Agencies have an "and operate" aspect to their mission statements.

He went on to discuss some of the responsibilities of SAMSO to lead into questions and problems as they face them and trends as far as one could perceive them.

- *Contractors performing on military installations* – he said that differences not only exist but also cause problems – visit requests (requiring SSNs), specific physical security requirements (alarm systems not meeting ISM standards). Incidentally, in connection with the SSN item, not on a military installation, he said that "It was really ironic that the day that [the Privacy Act] went into effect, the very first person that was stopped in the lobby and asked for his Social Security number was one of the Representatives that worked on the Congressional Committee to establish the Privacy Act." Not surprisingly, he refused to supply that information.

- *CNWDI* – As a user agency having programs dealing with *C*ritical *N*uclear *W*eapons *D*esign *I*nformation they had perceived the problem of failure to cover this topic in the *Industrial Security Manual*. He said this caused difficulties especially when an RFP was to be announced in *Commerce Daily* and a requirement for a Secret facility clearance with CNWDI capability was established. The DCASR Commanders were reluctant to certify on a non-existent contract. On a related point he touched on the ERDA [now DOE] Form 277 for processing a visit authorization as being a problem. He commented further that there were no instructions that informed a contractor that the Form 277 is also used (and is needed) to establish a mail channel (Ed. Note: a "mail channel" is required if it is expected that any documentation that might contain CNWDI is to be sent from a DOE-controlled facility to a DoD-controlled facility or contractor.) Mr Yokum went on to say about both points that he hoped DoD would provide:

- *Sponsorship of classified meetings* – In this connection Mr. Yokum said that when on a military installation it was really no problem. He went on to observe, however, that when, for example, DDR&E [now Under Secretary of Defense, Research & Engineering] requests sponsorship of a classified meeting at a hotel (not uncommon) and *hundreds* are in attendance that the chit-chat in the corridors, elevators, and rooms . . . is astounding. I know where one quest speaker at a lunch gets a lot of his information. All he has to do is attend one of these meetings in a hotel." By inference he was suggesting that yet another dual standard (Ed. Note: of *very* dubious merit) that should be forthrightly addressed.

- *Crypto Procedures* – He observed that the current variances among military departments is so wide that the problem is not small and needs resolution by DoD.

- *Proprietary Information and the FOIA* – He drew attention to some problems that exist in connection with contractor-prepared documents done specifically for a user agency – often under the user agency imprimatur – *i.e.,* no evidence that the contractor prepared them – commonly included proprietary information or other excludable information and the problem requires additional thought and guidance.

- *Foreign Nationals & Foreign National Visits* – The current emphasis on sharing the technical base with allies in Europe and the potential participation of foreign nationals in source selection boards likewise is a matter of concern to some contractors. There is potentially important proprietary information possibly included or revealed and it is another area requiring guidance.

Mr. Yokum touched lightly on a couple of other points; suggesting, for instance, that before one requests retention authority on older items one ought verify whether they're still classified. On another matter, he commented that ADP security was "the most pressing problem facing the user agency and the security program today." One of the aspects adding to the difficulties, in his view, was determining when an ADP system was user agency owned: many complex relationships exist and others are evolving.

Then he closed with a thought provoking discussion on what he termed Space Age Security. In brief, how does one protect classified information in space. How does one use patently unclassified facilities to launch patently classified payloads – referring specifically to the space shuttle program. He believes this to be a subject that NCMS should be addressing.

COST AVOIDANCE IN MANAGEMENT OF PERSONNEL SECURITY CLEARANCE

Arch F. Gady
Chief, General Acceptance Division
Defense Industrial Security Clearance Office

The work of DISCO as a part of the Defense Logistics Agency includes the processing of clearance requests for employees who may be used on a classified contract let by any one of the user agencies. I will attempt to cover points on how to improve the clearance program and reduce costs.

Every person assembled here today is concerned, I believe, about the ever increasing cost of food, clothing, automobiles, taxes and other day-to-day living expenses. Therefore, each person has a direct interest in reducing any government cost, even though small, since any such cost ultimately increases the defense budget, paid for by tax dollars, and adds to each person's cost of living.

DISCO's monthly workload average for December through February of FY 1978 showed:

ACTIONS

Type of Action		Number
Clearance Requests		9,502
Clearances Issued		9,215
Final Top Secret	594	
Final Secret & Confidential	6,159	
Transfer & Concurrent	1,959	
Conversions	502	
Terminations		8,984
Contractor Confidential Validation		4,531

Then, let us look at a few facts concerning rejects over the past three fiscal years:

REJECTIONS

Type of Submission	Percentage Rejected FY75	FY76	FY77
Formal PSQ-FPC (DD Form 48 or 49)	20.6	18.5	23.7
Resolutions of error without formal rejection	15.3	14.7	10.1
Total	35.9	33.2	33.8

The formal reject rate (where a letter was prepared rejecting the questionnaire, either parts one or three) was lower in FY 1975 than it was in FY 77. However, cases resolved by telephone were fewer in FY 77 and the total rejection percentage decreased from FY 1975 to FY 1977.

It would be well do display what errors cause rejection:

REASONS FOR REJECTION

Part		Percentage of Total Rejections
Part I		59.5
Employment Data	18.3	
Relatives	6.9	
Military Service or No.	5.9	
References	5.3	
Foreign Travel	4.0	
Other Relatives	4.0	
Date of Birth	2.8	
Part II		10.8
No Signature	7.1	
Part III		29.0
Arrest Details	18.2	
Medical Data	6.5	
Organization Membership	2.5	
Discharge Data	1.2	
		99.3

(Miscellaneous items not included in totals)

Now then, how can you help in cost avoidance, and thereby help reduce or prevent increase in your day to day costs? Look at the primary areas causing rejection; and to assist, here is a list:

- Be certain the Worksheet is complete.
- Proofread the smooth-typed questionnaire.
- Ensure that the employee reviews *typed* version of Part I.
- Ensure that the Security Representative signs Part II.
- Instruct the employee on how to complete the Privacy section – in private.
- Ensure that the completed questionnaire is signed by the employee and a witness.

Some comments about the points listed. If the work is incomplete it means additional work and time when typing. Every time a typist needs to put that questionnaire back in the typewriter it costs money.

Regarding proof-reading – too often we find the employee listed the information on the worksheet, but it wasn't typed. This is especially true about present employment. Remember that over 18 percent of the questionnaires were rejected because of employment data errors. Remember also that over 7 percent were rejected because the security supervisor did not sign Part II. As you are aware, a clearance is not issued until a *signed* request for clearance is at hand.

Help the employee understand the need for a complete questionnaire and review Part I in detail with him/her.

The completion of Part III – the Privacy Section – of the questionnaire causes many formal rejects. First of all, the employer should go over the questions with

the employee to explain what is required for each question. Discretion must be used to avoid being accused of violating the individual's privacy rights. There are a number of ways privacy can be maintained. These include placing a screen around a desk; using a separate room; or providing an area in a remote section of the office. To avoid costly law suits or lost time because of grievance actions, be sure the employee completes Part III in private.

When Part III is complete, Part IV is then signed and witnessed; the PSQ is placed in the envelope (signed across the back of the envelope by the employee) and dropped in the mail. Reproduction of any part of Part III of the completed PSQ is prohibited. If the PSQ is not signed by the employee, DISCO must ask for a new set and the one received cannot be returned because the privacy portion cannot be removed.

When processing a request for a conversion from military or civil service clearance to that of an industrial clearance, a copy of the notice of separation from the armed forces (DD 214) or personnel action form (SF 50) or variations thereof is required to accompany the DD Form 48-3. At the present time we are experiencing approximately a 20 percent error rate iin this area.

When you figure an overhead cost of $10.00 or $50.00 a day for a person in process for a clearance, it does not take an Einstein to figure the additional cost to you when a PSQ is improperly submitted. As you figure these additional costs, don't forget the mail time to and from your facility.

The DISCO is also trying to reduce the total processing item, and therefore costs, through reporting of investigations by automation. We are now transmitting those cases that are apparently "clean" via the computer to the Defense Investigations Services and the FBI; the results of all clean investigations are sent to DISCO via the computer from Fort Holabird. As a result, we have reduced our processing time by about eight days. We hope within the near future to have computer to computer response in the issuance of letters of consent on clean cases to further reduce the processing time and we hope this will be a reality within the next six to eight months. Concurrent with this we hope to be able to find some faster way of advising you, the employer, of the clearance approval for your employees. This could be through use of the telephone or teletype system. This is still in the planning stages.

In closing, I would like to leave this thought with you. All of us are faced with the problem of effective use of time. Doing the job over certainly curtails the time available for other things. Working together we should be able to reduce the reject rate and thereby reduce the time wasted in doing it over.

COMPETITION SENSITIVE MARKINGS

THE GOVERNMENT VIEW

M. Elizabeth Heinbuch
Office of the Deputy Chief of Staff
Research, Development & Acquisitions
Department of Army

The use of the marking "Competition Sensitive" has been a matter of dispute in the Department of Army for an extended period of time.

The term "competition sensitive" was coined years ago by the U.S. Army Materiel Development and Readiness Command (then the U.S. Army Materiel Command). It was intended as a caveat or marking to be used alone – or as an adjunctive marking with other protective markings – on documents relating to competitive prototype procurement. It was intended to alert the reader that the document, whether classified or not, contained cost, schedule, or technical information considered privileged by the contractor (AMC circular 715-6-73, 10 October 1973, "Procurement Instructions").

The provision for use of the marking "competitive sensitive" is not authorized in any DoD or Army directive or regulation. As a matter of fact we have just the opposite – the use of caveats such as "sensitive," "close hold," *etc.*, are prohibited. Primarily because they are not defined anywhere. Nobody really knows what they mean or how they're to be handled except the person who originates the caveat.

Strict adherence to the principle that any classified document shall be released only to persons properly cleared and who have a "need-to-know" will achieve the desired degree of control over the information. If it is deemed necessary to inform recipients of certain documents, classified or not, that release is intended only to certain persons designated by organization or function, then the appropriate handling instructions should be included in the body of the document or added as a narrative notation.

The DoD has provided guidance on protective markings for contractor privileged type information. DoD directive 5400.7, "Availability to the Public of Department of Defense Information" implements the provisions of 5 U.S.C. 552 as amended by public law 93-502 and prescribes a uniform policy for the identification and marking of documentary material or records which are not to be released to the public *for reasons other than security classification.* The marking used to designate this material is "For Official Use Only" (FOUO). Such information may be exempted from public disclosure under the Freedom of Information Act. Section VI of the directive provides examples of records which will be exempted from public disclosure. Examples include:

"Those containing trade secrets or commercial or financial information which a component receives from a person with the understanding that it will be retained on a privileged or confidential basis in accordance with customary handling of such records. Such records are those the disclosure of which would cause substantial harm to the competitive position of the person providing the information; impair the government's ability to obtain necessary information in the future; or impair some other legitimate governmental interest." An example being "commercial or financial information received in confidence in connection with loans, bids, contracts, or proposals; as well as other information received in confidence or privileged, such as trade secrets, inventions and discoveries, or other proprietary data."

In the Army, the Adjutant General has the responsibility for establishing policies and procedures for the protection of that unclassified information exempt by law from public disclosure.

The DoD directive has been implemented in the Army by AR 340-17, Release of Information From Army Files, and AR 340-16, Safeguarding For Official Use Only Information. AR 340-17 contains the same exemption from release to the public as I quoted from the DoD directive.

AR 340-16 contains provisions for the physical safeguarding of proprietary information – to include storage, handling, transmission, release, and destruction. Although that safeguarding does not mean *control* – it does mean *protection.*

It's stored with unclassified files when normal government internal building security is provided. If not, then it's stored in locked receptacles such as desks or files. There are restrictions established on release, and destruction is accomplished by tearing in pieces to prevent disclosure of contents.

An exception has been made to the Army's rule of three-year termination on the protective marking for information in the case that specific provisions of the Armed Services Procurement Regulation (now known as the Defense Acquisition Regulation) require different time-frames. The Adjutant General (TAG) has submitted to the Secretary of the Army a draft AR 340-17. It will be published as a supplement to DoD 5400.7R The new regulation will rescind the current AR 340-16 on FOUO and incorporate provisions for designation, safeguarding, and handling into one regulation – AR 340-17. But more importantly, the TAG is finally taking positive action on the prohibition on use of caveats such as "competition sensitive" on FOUO material. Let me read you one paragraph from the new regulation (para 4-100, General, FOUO)

> "With exception for technical documents that are marked with distribution statements in accordance with DoD 5200.20 and AR 70-31, Department of the Army records which contain FOUO information, but no classified information, will not contain any other adjunctive or substitute markings. If for valid reasons, unrelated to withholding such records from the public, it is necessary to limit access to the records to specific officials, or to impose more stringent measures than prescribed in this regulation for their protection, the instructions for such limitations and measures will be included in the records or in narrative form on sheets covering the records."

I hope that with the issue of the new regulation, the marking "Competitive Sensitive" will be put to rest – finally.

There's really no need for such a marking – we in government know that you in industry have information that you need to protect – and we have set up procedures to help you protect that information. Within government we consider that proprietary information generally falls into four categories:

- Research and development information.
- Production data.
- Marketing information.

- General business data (plans, performance, prices, and problems).

The industry practice of putting a proprietary type notice on a document is certainly helpful, in the right circumstances. On the other hand, this is one area where companies frequently tend to err by putting such a notice on every single document they send out. In my view, that tends to hamper your ability to protect anything in that it shows that it's merely a routine act rather than a conscious decision that somebody made based on that particular document and information. I understand the industry problem. Information is a very important commodity to us all – both industry and government. Any organization that does not have information to protect is not competitive. The industry problem is even more complicated because your threat is both external and internal.

The DoD feels that the key to procurement is competition. Along those lines, the commercial commodity acquisition program has been established in order to evaluate the overall DoD progress in our goal to achieve the ways and means to acquire, use, and support, commercial off-the-shelf products to meet our requirements. The theme of the commercial commodity acquisition program is "Commercial By Design."

I don't have the answer to the total problem – but I do know that the use of an unauthorized marking such as "Competitive Sensitive" is not the answer.

AN INDUSTRIAL EXAMPLE – THE ADVANCED ATTACK HELICOPTER

James M. Morgan
Bell Helicopter
Textron Corporation

Introduction

Doing the research for the foundation for the Competition Sensitive designation, I was unable to find a reference *per se* in either ASPR or the Army Procurement Directive. I spoke with people at the old U.S. Army Materiel Command and their feelings were that term Competition Sensitive was not founded on concrete regulations but rather on opinions and they would not take part in a formal discussion. So, you see, a contractor's Competition Sensitive Information has neither statutory nor regulatory basis. It is an administrative procedure used to protect the contractor's essential non-proprietary information as well as proprietary information.

As to rationale, background information seemed to suggest that there had been problems in prior proposals in that government employees had covertly or overtly leaked information between contractors. As a result, the Government felt that for the Advanced Attack Helicopter, a Competition Sensitive Information Security Guide would reduce or eliminate the leaking information by government and contractor employees. Such would apply to Bell Helicopter Textron and Hughes, in this case.

So, a competition Sensitive Guide was prepared by the Government and was used as the basis for safeguarding all documents, photographs, models and equipment and information pertaining to the Advanced Attack Helicopter. At the same time, the guide would not be interpreted as superseding DoD 5200.1-R as supplemented.

Meaning and Application

One may wonder what Competiton Sensitive Information is. It includes design details and other data of one contractor which – if disclosed to a different contractor in competition – would jeopardize and/or compromise each contractor's competitive position. As a matter of information, *Proprietary* information of a contractor furnished to the Government may never be disclosed to a third party without incurring legal material injury to the first party.

A contractor may develop information which is not considered a chattel but which is uniquely confidential and essential to the conduct of his business in winning a competition. In order to protect non-chattel information furnished the Government, the contractor marks the information Competition Sensitive Information.

It is reasonable to say that if these are the ground rules that the Government itself generates information that should be protected as Compeition Sensitive. Examples would include trip reports, meeting reports prepared by the Government on contractor progress, plans activities, problems or hardware features. Other examples might be pilot evaluation, engineering evaluation or cost evaluation of a competitive design which may be helpful to one competitor over another if disclosed.

Turning now to the problem of *control* of such information within the contractor facilities: using the categories established in the Government Guide, the originator of a document will be responsible for applying the marking at the bottom of each page or by

marking each paragraph that contains such information. In addition, the front cover (if any), the title page (if any), and the first page will be stamped or marked *Competition Sensitive.*

Documents marked Competition Sensitive must be stored in a locked desk or file cabinet. Information or documents so marked must be destroyed as classified waste. The transmittal of such information in some ways follows the procedure used for classified information – that is, double wrapped with opaque paper or envelope, inner envelope marked Competition Sensitive front and back, top and bottom, with address affixed to the inner and outer envelope. On the other hand it can be transmitted through the U.S. Postal Service by Certified or First Class Mail. Further, it can be hand carried.

The contractor must prepare a Compeition Sensitive Guide as must all sub-contractors. The sub-contractor guide requires review and approval by the contractor. The subcontractor must sign a statement regarding his responsibility under the program. In our last effort in this area, Bell Helicopter Textron had 65 sub-contractors who were under it. Each Bell Helicopter Textron employee had to sign a Security Statement and Certification and a Debriefing Statement when they left the program. Each sub-contractor employee also had to sign the same statement. I never did count all sub-contractor employee statements that were processed; I am sure there were volumes. All Government people involved also had to sign the statement or a similar statement.

Next was the development of a need-to-know list on all contractor employees who had signed the Security Statement and Certification; a part of such a requirement, as you would know, was the additions and deletions list so common to any need-to-know list. Accordingly, the list and changes thereto must be distributed to all employees on the list. It stands to follow that the sub-contractor has the same problem of maintaining records on Competition Sensitive Information.

Observations

As a result of all of this, the question arises: was it worth it? May I point out some pros and cons:

First – it reduced the possible unofficial leak by Government employees to one contractor or another.

Second – In the case of trade-offs – weight *vs.* survivability, for example – it keeps a given contractor's position fairly well protected.

Third – Was it worth all the effort and cost? I just don't know. I heard at least one executive say that even if we had had all the competitors' plans, we would *not* have changed our course.

Last – There is no question that it was an expensive procedure. I am certain that we would not want to go through another.

Questions and Answers

Question: Inaudible (Ed. Note: There were few questions that were audible. The answers that seemed to offer understandable comments are provided.)

Answered by Ms. Heinbuch: I propose that you protect it in one of two ways. If the contractor has affixed its proprietary-type notice to the item before you get it, that's fine. However, there is actually no reason why *you* can't mark an item For Official Use Only, or why you can't put a covering notation on it that says it contains information furnished you on a privileged basis and it's not to be released to another contractor or not to be released other than is provided for in a given regulation

Our feeling is that we, the Government, have provided the necessary mechanisms to protect such information. It was industry that reminded us that letting everybody along the way – like Darcom did years ago – come up with special markings like Compeition Sensitive, with a regulation pertaining only to them was bad. No other command in the Army was protecting it the same way and no other service would have any basis for understainding the intent or requirements.

Question: (Inaudible).

Answered by Ms. Heinbuch: The Headquarters Department of the Army, The Adjutant General – as noted above – has the primary responsibility for the Army in writing procedures and policies to govern how we're going to handle such information; actually who has the intelligence responsibility. We have all reached the conclusion that – and notifed Darcom to the effect – there is and will not be any other adjunctive phrase, competition sensitive, or anything else added to For Official Use Only-type information. There are only

three *classifications,* confidential, secret, and top secret. What we're talking about is a protective marking for unclassified information falling into one of those nine reasons listed in the law, and proprietary information happens to be just one of them. If you feel strongly about the situation do write to the Adjutant General.

Comment from Mr. Morgan: I want to make one comment that our company's been in existence for about 25 years and we've been extensively involved in major competition. This is the first time we've had a Competition Sensitive. I've asked some of our people about whether any of our information was "sold down the river," and that's what really counts. From the responses, I think we can say that we don't think we've been sold down the river on information that was made available to the Army or the Navy or the Air Force. So, I would say, unofficially without my president's permission, that we would be happy to live without Competition Sensitive and feel that we would get a fair shake.

Question: When you received this requirement from your contracting officer, did he pay you more money *in order* to take care of it?

Answered by Mr. Morgan: It's a contractual obligation. In our case it was charged to overhead costs, we did not "line item" that cost. So, we did not get paid for it *per se* but we did get some overhead costs which actually paid for at least some of it, but through a different funding section.

Question: The reason I asked the question is that most compartmented programs – and that is exactly the point – have provisions to pay for the additional security requirements imposed.

Question: Would the Army Headquarters like to know who in the Army is applying and requiring this marking documents and contractual material.

Answer: Yes.

Question for Ms. Heinbuch: You mentioned Army regulations. I have three things. The first is not a question. You mentioned AR-340, I believe it was, dash 16 and 17. Those would not be applicable in all cases because we have contracts with other than Army.

My second part has to do with Official Use Only. We have been under the impression that For Official Use Only is applied at the discretion of the government. We in contract houses are not entitled to use it, nor is it called out – unless directed by the contract – in the ASPR.

As a counter-proposal to what you're suggesting using For Official Use Only, would we not be better off to use the standard claimer in the ASPR?

Answered by Ms. Heinbuch: Certainly. I'm not saying that you in industry will start putting For Official Use Only on your documents. You'll continue the same way as you have been doing under ASPR, and with your proprietary-type notice. I can only speak for the Department of the Army and perhaps I'm not speaking very well for them. I don't know how the Navy or the Air Force does it. I assume certainly that they must have some regulation the equivalent of the Army's that implements this DoD directive. But, within the Department of the Army, and I think within the Department of Defense, once we get that document from you that falls in one of these categories of proprietary-type information, we will handle it as For Official Use Only, which means we will give it that protection it needs to exempt it from public disclosure.

Question (Continued): To elaborate just a bit more on that third point. It's very expensive in training programs and procedural efforts to utilize different methods for the three different user agencies or primary user agencies that we contract with. So all I'm really saying is that shouldn't we contractor people go strictly by the ASPR with our claimer clauses and try to avoid getting embroiled with a claimer for the Army, a different one for the Navy, something else for the Air Force, the Marine Corps, Coast Guard and so on.

Answered by Ms. Heinbuch: Certainly, and before I came I checked the ASPR. I checked the Industrial Security Manual, the Industrial Security Regulations, and every reference I could find, and nowhere in any one of those do they address Competition Sensitive or Competitive Sensitive. That's another example, by the way. Even when we're talking about that subject, to some people it's *Competitive* Sensitive. To some of us it's Competition Sensitive. The only reference I could find to Competition Sensitive – as I noted above – was in the Material Development and Readiness Command, and that was an old regulation that was dated 10 October 1973; an AMC circular that was titled, "Procurement Instructions," and it's been a source of dispute between the old AMC, Darcom now, and the Army for the last few years. Whether there was any legitimate reason to create the marking, there is not now and will not be.

PROPRIETARY INFORMATION, THE FOIA, AND THE ASPR

A. H. Bandy
Patent Counsel, Texas Instruments, Inc.

The purpose of the Freedom of Information Act is to insure the right of the public to obtain information about its government's activities and policies. To this end the act makes mandatory the release of government records. However, you will remember the act establishes nine potential exemptions:

- secret or classified matter;
- matters related to personnel rules and practices;
- statutory exemptions;
- trade secret and commercial or financial information;
- inter or intra agency memorandums;
- personnel or medical files;
- investigatory records;
- records prepared for regulation or supervision of financial institutions; and
- geological or geophysical information.

With the exemptions set forth in the law, both the agencies and contributors of information mistakenly assumed that adequate safeguards were provided as the following history will show.

In response to initial requests for information, government agencies honored its verbal agreements not to release, as well as regulatory provisions prohibiting release of information. They did this by determining that the information fell within an exemption and then relying on their agreement or regulation not to disclose. However, the requestors went to court to obtain release and in many cases were successful. As a result the government became more selective of the cases it would defend and the agencies had to furnish the information without giving the submitter notice unless the information was marked. When given notice the submitters began bringing reverse FOIA actions seeking to enjoin release. The submitters were not very successful before the courts either. The problem was how to proceed before the courts and what information had to be presented to establish a case in the first instance.

The early cases established limitations on the exemptions. Secret or classified matter was held to cover only matters specifically required by Executive Order to be kept secret. You have learned of the outcomes of some of these types of cases. Matters related to personnel rules and practices of an agency were held only to eliminate the need for a government agency to keep records that no citizen could be expected to call for. Statutory withholding was permitted only when the statute provided some basis upon which it may be administered. 18 USC 1905, which makes it a crime for a government employee to release trade secrets was held no basis to deny release, and has now been amended to exempt from its scope trade secrets released under FOIA. Inter agency and intra agency memorandums the courts said must pertain to the deliberative decision process. Personnel or medical files could only be withheld when disclosure constituted a clearly unwarranted invasion of personal privacy. Documents classified as investigatory files the court said are not exempt *per se*. Disclosure could only be withheld to prevent premature discovery by defendant in an enforcement proceeding.

The submitters and appellate courts were not satisfied with these decisions but could offer nothing better. An administrative judge hired by the Federal Power Commissioner to decide a request for a contract proposal came up with the approach used today. The administrative judge using the history of previous release of information acts – the legislative history and court decisions – established that any disclosure consideration must recognize that:

- the release of government records is mandatory;
- the exemptions are permissive only;
- the appropriate exemption must be selected; and
- facts submitted to show that for this particular request the private interest outweighs the public interest for disclosure (Planning Research Corp. vs. Federal Power Commission 55F 2nd 1970).

How do we balance the interest? Well, for example, a request for a procurement proposal falls within the trade secret exemption (4th exemption). *For release*

denial one must show that release could cause substantial harm to the owner's competitive position or impair the agencies ability to obtain necessary information in the future (National Parks and Conservation Assn. vs. Morton 498 F 2nd 765).

What can we expect from the agencies in light of these decisions? NASA has taken the lead and amended its procurement regulations. First, NASA states its need for proposals uninhibited by the release possibility. It states that its use of proposals is only for evaluation purposes. It recognizes that although proposals might not include trade secrets they could contain commercial or financial information which if released could cause substantial harm to the owner's competitive position or impair NASA's ability to obtain necessary information in the future.

Secondly, NASA offers all the protection permitted under the FOIA. However, NASA warns that:

- proposals might be agency records;
- agency records must be furnished unless exempted;
- It cannot guarantee that a particular portion of a proposal would be exempt;
- It will provide notice to the owner of proposal data before releasing any portion; and
- commercial or financial data need not be marked, but where it is the practice of offeror to treat commercial or financial data as a trade secret offeror may mark it with the notice NASA provides for technical trade secret information. (as shown below)

NASA NOTICE

"Data on pages of this proposal constitute a trade secret. It is furnished to the Government in confidence with the understanding that it will not, without permission of the offeror, be used or disclosed other than for evaluation purposes; provided, however, in the event a contract is awarded on this porposal the Government may obtain in the contract additional rights to use and disclose this data."

Texas Instruments is using the legend of ASPR 3-507.1 for every page of a proposal. The legend is similar, as you will note, to the NASA NOTICE.

DoD LEGEND

"This data, furnished in connection with Request for Proposal No. , shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate the proposal; provided, that if a contract is awarded to this offeror as a result of or in connection with the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the contract. This restriction does not limit the Government's right to use information contained in the data if it is obtained from another source without restriction. The data subject to this restriction is contained in Sheets , (1966 Dec.)."

The ASPR instructions authorize use of the legend for design or concept information or financial and management plan which the offeror does not want disclosed to the public.

However, the Office of Federal Procurement Policy has adopted a draft policy which, from the advance information, appears to be patterned after the NASA procedures, and it is emphasized "that the guidelines would in no way relieve a procuring agency of its responsibility to examine individually the facts in each case before making a determination to withhold or release." So offerors will have to be prepared to prove that protection of the private interest outweighs the requesting party's public interest. The offeror might not have time to do much spade work, because the Government has 10 days from receipt of a request for information to make a decision. Failure to make a decision in that time is an exhaustion of the requestor's administrative remedy and he may sue without the agencies' decision. What can be done if the procuring agency decides to release? The offeror can bring a reverse FOIA action. Whether this can be a new trial is presently before the Supreme Court for decision. The case is Chrysler vs. Brown.

To summarize the development, the logic of the early determinations was (1) trade secrets and commercial or financial information are exempt from the act (2) proposals constitute trade secrets and commercial or financial information (3) therefore all proposals are exempt. The logic today is trade secrets and commercial or financial information *may* be exempt from the act depending on whether the private interest outweighs the public interest.

Thus, for the foreseeable future, when an offeror submits a proposal there is no assurance that it will not be released in whole or in part. I found the Planning Research Corporation case interesting in that the administrative judge determined the private interest to be the protection of some 1200 pages of computer trade secrets. The pages included 20 years of the company's computer development. He found the public interest to be expressed in the Federal Procurement Regulation prohibition against public disclosure of proposal information. Had the information been categorized as trade secret information and release denied because of the regulation the decision probably would have been reversed.

The question now seems to be how much harm constitutes substantial harm to one's competitive position. This is a judgment call, judgment calls beget arguments, therefore I predict a stormy future for FOIA.

Questions and Answers

Question: Have you explored this problem in the international arena? For example, in the DoD Industrial Security Program, we execute patent agreements for the United States with several European countries, as I'm sure you're aware. Has this been addressed in the same light?

Answer: I am not familiar with that and so I can't answer your question specifically. I am familiar with a case which is of vital interest right now to the Export Control Regulations and I'll describe the case.

Siemans, a German corporation, has a trade company in San Francisco. They purchased the ion beam implantation machine and were trying to ship it to Moscow when the customs people caught it. They did not have an export control license. So they brought criminal action against Siemans in San Francisco. The defense attorney brought a discovery action for five or six publications, two of which were Texas Instrument documents, but they were not marked. We just furnished them pursuant to the contract but did not mark them.

The court refused discovery. So, Siemans has brought a Freedom of Information Act in the district court requesting the documents. The government is on the hot seat this time and they are looking into the question of releasing the documents. What they're trying to protect is the lead time that it would take Russia to develop the ion beam implantation machines.

Now, the question I guess since it's brought as a statutory exemption is whether the export control regulations provides an adequate guideline on which they can deny release. If Siemans can get those things under the Freedom of Information Act, I would assume that the export control regulations are going to go out the window.

MULTI-NATIONAL CO-PRODUCTION VISITS AND OTHER CHALLENGES

Robert Behr
Foreign Disclosure Policy Officer, Aviation Systems Division, AFSC

The Program Office View

Foreign Disclosure Policy may, at passing thought, seem only remotely related to classification management. Yet, indications are that these functions will become more and more related. Therefore, a full understanding of the respective areas of interest and responsibility can be only beneficial to the program. In the NCMS Journal (Vol XII, No. 2) covering 12th Seminar, some points were covered then that will be examined further. Primarily these are:

- Co-Production
- Export Licenses
- Visit Procedures
- Security Clearances
- Protection of unclassified data overseas
- RFPs to foreign countries
- UN/Canadian/NATO review of Defense Programs.

From the earlier presentation you will remember the F-16 fighter/interceptor aircraft co-production program was presented along with some of the major problems facing such an endeavor. While two years ago one might have imagined the program to be unique, in my opinion co-production no longer will be an isolated occurrence. I firmly believe that any major weapon sale today will involve a co-production effort as long as the buying country has the industrial capability to manufacture part or all of the weapon system. Co-production may take several forms such as:

- off-set

- licensing arrangements
- subcontracting.

No matter which form of co-production is chosen, all of them will have an impact on industrial security, classification and foreign disclosure. *Contractors* please remember, are involved to such a degree that it makes them, for all practical purposes in many instances, *the* prime agent responsible for security and foreign disclosure. Particularly is this true when a licensing agreement is arranged.

An example, not revealing an unknown, is the sale of F15s to Japan. For all practical purposes the sale is a commercial sale between the Government of Japan and McDonnell-Douglas. An export license has been issued that would cover issue of the necessary documents, know-how, and components to Japan. But, what about foreign disclosure? A question is whether Japanese industry has available the capabilities and capacities already or whether we *are* shortening their development time and cost. If you will recali, the Air Force, in the case of foreign military sales, issues a Delegation of Disclosure Letter (DDL for short) which becomes the primary document governing releasibility or nonreleasability of specific *information.* In the case of licenses we would have, of course, no DDL since the arrangements are between a private contractor and foreign industry. The problem of disclosure, however, does not go away and so what takes place is that the Air Force issues a DDL anyway and the DDL will be inserted into the license by reference. In practical terms this means that the contractor will have an export license. However, it will require him to work closely with Air Force foreign disclosure personnel to insure the orderly release of those data authorized and prevent release of those not authorized under the DDL. This arrangement will require that we streamline the operations and arrange for maximum redelegation to DCASR or AFPROs to avoid delays in releasing information required by the foreign customer. In addition, we will make sure that the DD Form 254 also will reference the DDL thereby insuring that all elements, government and industry, are tied together on a common cause.

Let us turn now to the preparation of and responsibility for DDLs. At this time, to the best of my knowledge, there is only one DDL for which the Air Force has tasked the Foreign Disclosure Policy Officer to be responsible for and to be involved in the industrial security program. In my opinion, this will change rapidly. Those of you who are industrial security officers should make every effort to get acquainted with the foreign disclosure policy personnel in the respective military organizations to insure a smooth working relationship.

The problems which have arisen in co-production efforts require total cooperation between industrial security and foreign disclosure personnel. Let me cite only a few examples of the problems we have experienced in the F-16 Program. The first of which concerns visit procedures. You are all aware that most foreign visits require an approval by DoD. The number of visit clearance requests submitted by the European co-producers to visit U.S. contractors had assumed the astronomical number of almost 900 for calendar year 1977. We work, as you know, only on blanket clearances whereby all clearances are good for a complete calendar year. This too has saved much time and work. However, of these 900 clearance requests, approximately 450 were simple amendments adding or deleting a single name. This posed an unacceptable workload to the processing military organizations. At my suggestion, the Air Force agreed to radically change the procedure whereby all amendments to existing blanket clearances are sent directly by the foreign Embassy to the security officer of the U.S. Vendor concerned. This has reduced the time from approximately 2-3 weeks of processing an amendment to about 5 days, and the workload factor was cut in half. We are still experiencing Pentagon concern over the fact that second and third tier vendors in Europe are submitting visit requests to go to U.S. contractors; yet we have no record of the contractual relationship between the European Vendor and the U.S. contractor. Next year we will try to solve this problem by having only the major European Vendors submit a visit request to which all the second and third tier vendors "Request for Visits" are attached. Thus, the Foreign Liaison Division in the Pentagon would only have to process one complete package per major foreign subcontractor.

In the opposite direction, that is U.S. travel to the foreign countries, it may interest you to know that the industrial security officers in the four European countries, which are co-producing the F-16, have refused to accept a "Company Confidential" clearance. They are maintaining that no U.S. contractor personnel without a DoD clearance shall be permitted to enter their facilities. In addition, they request that contractor personnel which have no clearance be either restrained from travel or obtain a government clearance.

I do not have to explain to you what this will do to the number of U.S. contractors involved in the F-16 Program. We had to act rapidly and decisively to overcome this handicap and I am happy to say that we were able to do so. The Defense Logistics Agency has given us their full cooperation and authorized DISCO to process DoD clearances for all U.S. personnel required to visit European co-producers.

One additional problem concerning foreign visitors to U.S. contractor installations which we have been unable to make the Europeans understand is the term of "Foreign Representative." I have been unable to make them understand that if a European contractor hires a U.S. company to represent them that personnel from that company will also require a visit clearance the same as the Parent Company. This requirement seems to the Europeans so different that it will take somewhat more education to make them understand and adhere to it.

Let me elaborate on some of the other problems relative to co-production effort and illustrate it by telling you the saga for the protection of unclassified data. There is, as you know, no DoD regulation I know of in the U.S. which requires the contractor to protect unclassified, unmarked information. Yet, we are shipping millions of dollars worth of unclassified production data to European countries without the slightest assurance that this data receives even the minimum protection. Clearly, something had to be done. What we did in order to provide protection was to request the Europeans to treat such data as "controlled data." Since the Europeans have no category of "controlled data" as we have in the United States under AFR 80-45, they declared all F-16 unclassified production data to have a "NATO Restricted" classification. Then they directed their vendors to protect the information accordingly. No sooner had those directive been issued when the U.S. prime contractors were requested to provide additional funds for the "safeguarding of unclassified information." This, of course, was not the intent at all and we tried to explain this to the Europeans. We did not succeed. Next, they requested that we mark every document "FOR OFFICIAL USE ONLY" – a physical impossibility with the thousands of documents transferred to European co-producers. Then, they requested us to differentiate between that unclassified data which required protection versus that which did not. The final result of this long drawn out problem is that we finally explained to the European security officers that we would appreciate it if they would "treat" the data as "NATO Restricted" without, however, any insertion of markings such as "FOR OFFICIAL USE ONLY" or "Controlled Data.", etc. We think that we have now succeeded to receive protection for our data without additional cost to the program.

And yet another area of interest related to the Security Classification Guide for the F-16 engine. The Security Classification Guide lists two items as being classified, while all other components are unclassified. What the security officer of the country co-producing the engine did was to instruct the company to request funds to build a 6 foot high fence and to install appropriate doors with locks on their facilities in order to safeguard the classified information as listed in the Security Classification Guide. What they totally overlooked was the fact that neither of those two items would ever go to the foreign contractor. The classified items were only released to the government concerned and in no way to the contractor. You would think that a security officer would take the time to inquire about this aspect before directing a company to construct physical security safeguards – no so. It took the combined efforts of my office as well as the F-16 SPO to assure security personnel overseas that no fences or locks or any other kind of physical security measures were required to protect classified data (of course, physical security may be needed for other reasons). One must be cautious when transferring a Security Classification Guide to a foreign participant. The example cited reminds that Security Classification Guides often can be misunderstood and may be abmiguous to the uninitiated; they require many years of association to understand fully how they are to be read, interpreted, and implemented.

One of the problems – perhaps best understood by this group – is the fact that a program such as the F-16 Program, does not have even one fully qualified security officer either in the U.S. or in our office in Europe. During one of our annual meetings the point was made by the European security personnel. They could not understand how major programs with either co-production or licensing arrangements did not have security personnel assigned to them. In my personal view, I agree fully. I have taken steps personally to bring this to the attention of appropriate AFSC personnel. I know that steps now are being taken to see whether a security officer could be assigned to our F-16 European Office. I don't know if it will succeed, but I submit to you that security is an integral part of any major international program. It will take all of us to educate our management because all too often security is taken for granted. Such duties and responsibilities are given to persons without background and

training. I think NCMS could play an important role in convincing DoD of the necessity of assigning competent persons to the information security aspects of major international programs.

As to potential problems coming into view, steps are being taken to allow contractors of our NATO Allies to compete equally with U.S. contractors. Clearly such a policy would affect Foreign Disclosure areas as well as be of interest to U.S. contractors. We must make sure that, should a UK or Canadian contractor, for example, choose to bid on an Air Force contract that no foreign release problems will impede his participation. So, there is an elaborate process to determine whether a foreign release problem exists before advertising in the *Commerce Daily*. If there is, only top management in the Pentagon is authorized to make a final determination on whether a foreign contractor should be excluded from bidding. Clearly the concept applies to subcontracting with foreign industry and should be a great interest to industry represented in this Society. I suggest that you look at this aspect as you are awarded contracts by DoD.

THE CONTRACTOR'S VIEW

B. K. Bradfield
Manager Industrial Security
General Dynamics Corporation

As Mr. Behr pointed out, the F-16 program is a co-production program – in every sense of the word. A wing of the F-16 is made over there, the Centrifuge here; the horizontal stabilizer in yet another place. The various parts come together in one place to be mated on some airplane. That aircraft may be delivered in Europe either to our allies or the U.S. force; or it may be delivered to U.S. forces elsewhere.

The landing gear, the aileron, flapperons, the speed brake, are all things made in one or another of the five countries. There are three production lines going inside the five countries. The picture is, to say the least, very complex. In such a circumstance you can imagine the response times that are required for visits, for example. General Dynamics is the prime contractor. We are responsible for meeting schedules over there and here; for quality control, transportation, shipping, receiving and the like, spread out over half the world.

We recognized long before the contract was let, that visits were going to be quite a problem. And we were promised that the visit program would be modified, that the government was really going to make things easy to get people back and forth. Well, that didn't happen in fact. Mr. Behr has explained some of the things he instituted and he really saved the day for us as far as visits to other contractors go. Procedures were established so that visits to contractors are handled directly through DISCO (Mr. Gady) and Mr. Behr.

However, if we are going to go visit a government organization over there, or a military organization, then that is quite different and difficult. To give an idea of the chain of events, after we get the visit request typed, it goes to our local AFPRO. It is processed out of the local AFPRO to CMD, CMD processes it to AFSC. AFSC then processes it sometimes to headquarters USAF, other times directly to the government concerned.

I understand that the request goes through something like 27 different people's hands before it gets out of this country and is sent to the country to which it's going. The lead time is atrocious. Production in all three countries has not peaked yet; in fact, it is just now beginning to get warm. I anticipate that we are going to have all kinds of problems when we need to visit government organizations. However, the contractor to contractor procedure right now is most important and it seems to be working very smoothly, with the help of Arch Gady and Bob Behr.

Now I would like to turn to another challenge that is just around the corner. We have, of course, recognized for the last two years the question of shipping classified hardware. There are no more than six pieces of classified hardware on the F-16 fortunately and they are at the confidential level.

But, these six pieces of hardware have to be transported from here to Belgium and to the Netherlands. Once they get there, they are tested. If an item doesn't check out, if it fails for some reason, it has to go for repair to a contractor plant located in the Netherlands at Falker. How is the equipment going to get from Belgium to the Netherlands and back to Belgium again. Remember that contractors are prohibited from hand carrying classified hardware across international borders not to mention all the other restrictions. Access to the hardware is only during normal daylight hours for instance.

The government has already told us they can't support the schedules that are required under this program. But, they also told us, don't worry, something will be done. Well, we are just a very short time away from delivery of the first items. We had a meeting at

General Dynamics recently with about 25 people who came to discuss that particular problem. I don't know at this time, what is going to be done about it.

The government's proposal to General Dynamics was this; because the government cannot support the schedules, General Dynamics give us a management transportation plan on how you propose to get the classified hardware back and forth across international boundaries under current regulations. Obviously, it can't be done. We can't get across the border, and that it what we told the government. They replied by letter saying, that we were non-responsive to their first letter. So, they came to discuss the problem – for two solid days. I think now the appropriate people are aware of just what our problems are with the *Industrial Security Manual.* The industrial procedures and regulations are different from what the government would do.

Recently General Dynamics purchased a Convair 880 and outfitted it strictly for use between here and Europe or Iran, or to other countries that might purchase the F-16. The government said, well there is the obvious answer. You load the hardware on the 880 and the government will get some kind of a waiver to let you fly it over and offload it and meet your schedules.

Well, that is fine up to a point. However these are likely problems. What happens when that 880 isn't flying because of some mechanical problems. Presuming a waiver to hand carry, it to Europe, what do we do with the classified hardware when we get there? Remember that classified material can only go government to government. The Europeans have already said, look, it is your responsibility to get the material to us. So, we land in Belgium, how do we get the material to the Netherlands. How do we get it to Norway or Denmark? We are crossing borders again. Who is going to be there to meet us? Then, what happens if the 880 is diverted because of weather or some other reason, and we have to land somewhere else? We have classified hardware onboard. What about customs? All of these things are problems. And, they are problems that no one wants to face now because they are not immediate. But believe me, they can be costly later if proper plans are not made.

I don't know the answer or what the government is going to do for us. We can't act as an agent of the government in all of these ways. Because of the customs problems, etc. One might think that an obvious solution would be to deliver the classified hardware to the Belgian Embassy. Then they could put it on a Belgian aircraft and fly it over. However, the other three countries have said already that they would not go to Belgium to get their material. Further there is no assurance that Belgium would agree either since the procedure obviously would cost them money, and wasn't part of the contract.

So these are challenges. They are interesting problems that will keep your mind limber trying to solve them. Perhaps by next year, if we are still in business, I can report on how this has worked out.

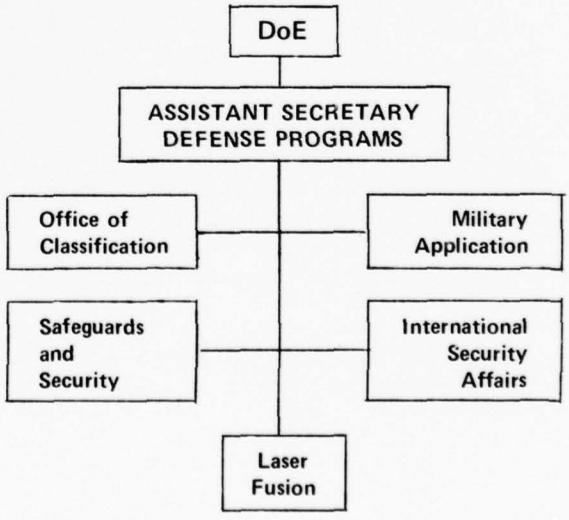
CLASSIFICATION MANAGEMENT AT THE DEPARTMENT OF ENERGY

THE HEADQUARTERS SCENE

Esther "Jill" Ellman
Office of Classification DoE

As some of you know, the classification system at DoE is highly centralized, and it seems to have worked well for us over the years from its onset under the AEC, then through ERDA, and on into DoE. We realize the approach would not work well for everyone but we would like to share some of our thoughts on this kind of organization and the problems as we view them.

First, we might explain where classification is placed in the DoE structure. In addition to the various regulatory, administrative, advisory and support organizations, the DoE has six major line organizations each headed by an Assistant Secretary. One of these is Defense Programs and is shown below.



Two points about this structure may be unusual. First, the classification and security functions are in separate offices. Often these responsibilities are combined. However, in DoE classification is a separate function. The Office of Safeguards & Security is responsible for personnel clearances and the physical security of classified information as well as being re sponsible for the safeguarding of nuclear materials.

Second, we are part of a line organization rather than being under a staff office, such as Administration or Policy or in the Office of the Secretary. In DoE this works out well because most of the classified information generated relates to Defense Programs, while much of the rest of the department is involved in totally unclassified efforts. However, when the circumstances differ there are advantages to being in a staff organization, for instance when one is responsible for overseeing activities in other line organizations. I might remind that under the AEC, we *were* under the Assistant General Manager for Administration.

The major responsibilities of our office are:

- **Develop and recommend policy for classification and declassification of information for Secretarial approval**
- **Interpret classification policy through issuance of guidance, rules and procedures**
- **Coordinate and implement policies through administration of DoE's classification and declassification programs**
- **Coordinate classification matters with other agencies and foreign governments**
- **Review all classified material requested under FOIA**
- **Administer DoE's compliance with Executive Orders,**
- **Represent DoE at the ISOO level**
- **Evaluate and improve DoE's classification program.**

As you can see, one of our major jobs is to develop classification policy and issue guides. Guides will be required under the new Executive Order. Although we have been in the "guide writing" business forever because of the law, nonetheless we will have new guides to write. We feel that some DoE activities may not be adequately covered by existing guidance, *e.g.,* intelligence and foreign affairs. Recently, we have been working on guidance for our nonproliferation activities. That task has been a real education. As many in the Society know, it is much easier to write guidance for specific technical information when one can establish that Part A is classified Secret and Part B is Confidential. It has proven *much* more difficult to write useful guides for nontechnical areas. We sympathize with agencies like the State Department, now facing the prospect of writing major guides. Another point to make before leaving our responsibilities is that our staff reviews all classified material requested under the FOIA or the Mandatory Review provisions of the Executive Order. The Director of Classification is the denying officer, when necessary, even if the document in question was generated by another Headquarters Office or by a DoE field organization. The Office of Classification interacts with all components of the DoE organization. It is the focal point for all classification and declassification activities and provides classification guidance to all offices both Headquarters and Field; we approve all guidance used by our contractors.

We have been accused of sitting in our ivory tower 2000 miles from the scene of action and making classification decisions. We really do try, however, to have wide participation in the development of classification policy and guidance. Whenever we are preparing to establish classification policy for a new program or to change policy or to create a program guide, we request input from the program managers, contractors, other agencies, other governments, *etc.* Often we set up a working group to draft the classification guide that will spell out the policy.

Turning to that point, which organizations are requested to participate in drafting a guide depends on the kind of guide being drafted. There is a hierarchy of guides in DoE.

- Central policy guides. About 35 *Program* guides (each specific to a DoE program such as gas centrifuge). About 400 *detailed* Local guides (used by our field organizations and contractors).

Clearly a different purpose is served by each. The policy guide is intended to provide broad policy statements on what should be and what should not be classified under the various DoE programs. Traditionally, such a guide has been approved by the head of the organization and is coordinated with

other agencies and with the British and Canadians. The purpose of that kind of guide is to set forth the differing subject areas and their lines of classification. No classification levels specified. Therefore, this guide is not really a "working" guide. It is intended to be used as a basis for more detailed guides. We are planning to revise our policy guide, mainly to add sections on areas no previously covered. We anticipate this project will take over a year for various reasons, one of them being the number of organizations that have to concur.

- Program guides are approved by the Director of Classification and must be consistent with the basic statements in the DoE policy guide. Many of these guides are coordinated with other agencies; in fact, as many of you who are involved in DoE nuclear weapon programs know, some of our program guides are actually issued as "joint" guides and the same guide topics are used by both agencies involved. We think this is a good idea and one that could possible be extended to other areas where there are programs cutting across agency lines, e.g., intelligence, disarmament, foreign affairs.

- Local guides are the "working level" guides which are used by our contractors in making day to day classification decisions.

Remember *all* guides are approved at Headquarters. There is a real danger in dictating policy from Washington and, in fact, there may be some truth to the prevelant belief in the field that Headquarters never *really knows what's going on; however, we count on our field offices to keep our feet on the ground.*

THE FIELD OPERATION

R. Richard Fredlund, Jr.
Director, Classification & Technical Information, ALO

When one moves to the field from Headquarters some aspects change. The Albuquerque Operations Office (ALO) is DoE's *largest* Field Office. In it the Classification and Technical Information (C&TI) Division is responsible for three basic functions; namely, classification, technical information, and administration of the Freedom of Information Act. Headquarters participation in the drafting of the forthcoming Executive Order with its expected changes has caused it some concern about its impact on Classification program resources. There is, of course, a lot of good news expected from the new Order. However, even the best of plans may have some potentially adverse effects. For instance, I'm sure that you've heard the good news about the deliverance of the Children of Israel from Egypt, but perhaps you haven't heard the whole story. Here's what probably really happened . . .

You'll recall that Moses was doing some research into alternative energy systems, specifically, nonconsumable burning bushes. Well, as he was testing one of his nonconsumable burning bushes one morning, God spoke to him from the bush, and said something like this: "Moses, I've come to give you some good news and some bad news." Well, Moses was pretty excited about this. He said, "Gee whiz, God, it's about time. We really need some good news. We have been having a hard time with these Egyptians lately. After all the other indignities that they have visited upon me personally, now they want us to make bricks with no straw. I mean it is really terrible! We *need* some good news, so how about giving me the good news first, God." And then God said, "Well, very well. I'll tell you what the good news is first, Moses. I've decided to deliver the Children of Israel from Egypt. What I'm going to do is that I'm going to visit all manner of plagues upon the Egyptians. I mean like locusts, hail, drought, death and assorted other unpleasantries. I'm going to get them so upset they'll be happy to wish the Children of Israel 'Godspeed', so to speak. And furthermore, if, after they let you leave, Pharaoh changes his mind, and decides to come after you, don't worry about a thing. I'll just part the Red Sea and you can walk across. If the Egyptians try to follow you, I'll drown 'em like rats! Don't worry about a thing, Moses, I've got it all under control. All you have to do is to just lead the Children of Israel right into the Promised Land. Milk and honey and all that sort of thing." Now Moses was pretty excited about all this. He said, "Gee whiz, God that is just about the best news I've heard this year and it has been a year sorely in need of good news. But you said something about some bad news." To which God replied, "Well, Moses, yes . . . there is this little bit of bad news. You see, you're going to have to write the Environmental Impact Statement and you have to paragraph classify it!" So you can see blessings tend to come in mixed packages.

Assuming that these and other concerns relating to the new Exective Order can be worked out, perhaps we'll be able to return to our more prosaic and familiar functions. In the DoE, we see the areas of classification and technical information to be parallel. This results partly from the fact that they are so

identified in the Atomic Energy Act, *i.e.,* the Atomic Energy Commission and its successor agencies are charged with disseminating as much technical information as is possible consistent with the common defense and security, while classifying the minimum amount of information required to assure that security.

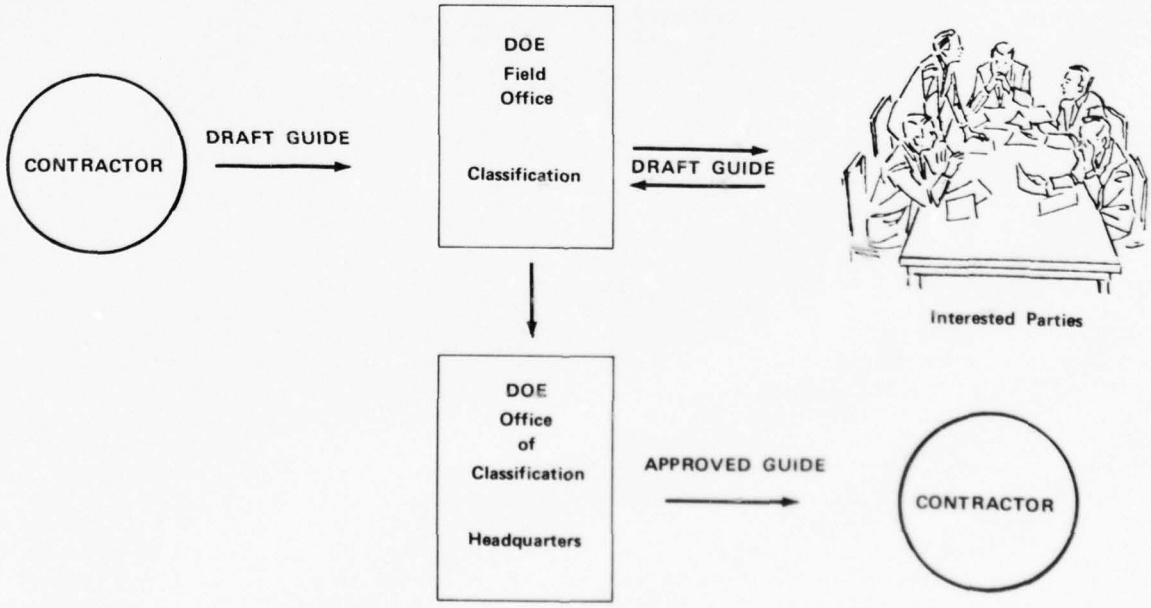
In the classification and technical information areas, Albuquerque is primarily responsible for the appraisal and oversight of the programs of seven contractors in eight states. They are:

Los Alamos Scientific Laboratory	Los Alamos, NM
Sandia Laboratories	Albuquerque, NM Livermore, CA Tonopah, NV
General Electric Neutron Devices Department	Clearwater, FL
Monsanto Research Corporation	Miamisburg, OH
Bendix Kansas City Division	Kansas City, MO
Rockwell Rocky Flats	Denver, CO
Mason & Hanger-Silas Mason Company, Pantex Plant	Amarillo, TX

The relationships that exist between a DoE field office and its principal contractors is similar to that of DoD and most other Government agencies. Administrative line control is separate from program or operational control. Further, organizational relationships are similar in nature to those which exist between DoE Headquarters and its Field Offices, as Jill Ellman discussed earlier. An interesting and perhaps unusual feature of these relationships relating to classification is that the lines of communication are rather short; from the Director of Classification at DoE Headquarters to the Field Classification Officers, directly to the contractor Classification Officers and thence to the various technical program applications. So that in matters of classification policy the Classification Officer at either a Field Office or any of the contractor organizations has a great deal of latitude to deal directly with those actually involved with an immediate problem.

As you will remember from "The Headquarters View," the greatest number of classification guides in DoE are "local" guides. A majority of these are drafted by the contractor responsible for the particular program or aspects of it to be program addressed by a guide. The figure portrays a simplified representation of what sometimes becomes a rather complex process.

When an ALO facility begins work on a new program, the contractor's classification officer (in cooperation with the technical organizations involved in the program) drafts a local classification guide, coordinates it within his or her own organization and possibly also with other potentially affected DoE contractors. Then, the draft guide is reviewed for approval by ALO Classification and Technical Information Division. It



PREPARATION OF LOCAL GUIDES

considers conformance with established policy and decides what, if any, further coordination is required; either with Program Divisions at the various Department of Energy Field Offices, or DoE contractors. During review if any differences of opinion arise or suggestions for improvement are made, they are coordinated.

Then, the guide is submitted to the Office of Classification, DoE. One may comment that, because of the technical expertise brought to bear in the preliminaries, frequently the guide will be approved by Headquarters as submitted (Ed. Note *Cheers*). However, even if this occurs, we believe that the process of Headquarters approval is important. The DoE centralized structure requires one office: *i.e.,* the Office of Classification, to maintain an overview of all DoE classification guidance, ensure that the many local guides prepared are consistent with each other, and, in fact, accurately reflect classification policy decided.

Because this system has central control features, it is infrequent that local classification guidance is inconsistent with policy. Not a small feat considering the large number of guides published and the fact that commonly many DoE contractors participate. As you might rightly conclude, a substantial amount of resources is required to operate such a centralized system. One may turn then to whom does DoE consider eligible to determine applications of guidance.

Along with a passion for consistency and, one hopes, consistent with it, there is a philosophy of "personal responsibility", *i.e.,* we want to know precisely *who* is assigning the classification to any given document. When only designated persons assign classification then it is an easy matter to determine exactly who needs additional classification education when mistakes are made. By limiting those individuals authorized to apply classification markings to a document to those who have a demonstrated competence in the subject matter of the document, we believe that we minimize the possibility of errors in classification. Moreover, limiting the number of persons authorized to apply classification markings within any organization, also limits the number who must be educated with respect to changes in classification policy.

Obviously, this approach has a number of drawbacks. We believe the benefits of the system are substantial, but it requires a substantial amount of classification program resources; both administratively (in keeping track of exactly *who* the authorized classifiers are) and operationally (in identifying and educating replacements for authorized classifiers who leave for whatever reason).

One of the reasons for the adoption of the DoE authorized classifier system was the traditional philosophy of AEC → ERDA → DoE that it is extremely difficult to make classification guides precisely definitive. It follows that, if consistency in the application of the guides is to be achieved, we must ensure that those persons actually applying a guide to a specific technical question are "skilled in the art" of classification as well as technically competent in the areas to which the guidance is being applied. This is not to say that we necessarily limit the dissemination of classification guidance to only those persons who are authorized classifiers. On the contrary, we attempt to ensure wide dissemination of classification guides to those persons working in potentially classified areas, who may have a necessity to identify classified information. In this way, we hope to alert the technical population to information requiring protection on or with which they may be dealing. They can discuss the matter with an authorized classifier. Because of this philosophy of "personal responsibility," classification guides are not used as classification authorities in the DoE under Executive Order 11652.

Considering the forthcoming changes expected in the new Order, our current plans are to continue our philosophy of personal responsibility. But, consistent with it, to drastically limit the number of DoE and DoE contractor personnel assigned "original" classification authority. Simply stated, we would propose to give the few *key* authorized classifiers at a location "original" classification authority. All other "authorized classifiers" at a facility would then have "derivative" classification authority. We *do not* at this time plan to extend authority to apply classification to information or materials to any person *not* specifically authorized either as an "original" or "derivative" classifier.

We recognize that this policy is a great deal more stringent than is required by the words of the draft Order. However, we believe it is certainly consistent with the spirit of the Order and with the DoE philosophy of ensuring that each time a document is classified, a conscious decision to do so is made by an identifiable person, competent in the technical subject matter of the document and familiar with current classification policy in the area.

In summary, the DoE classification program is highly structured, centralized, and has heavy emphasis on personal responsibility for those making classification policy or individual classification determinations. Because of our success with this approach within the DoE, and because the relatively small size of the DoE makes such centralization possible, we plan to continue this basic philosophy and structure under the new Executive Order.

THE DEVELOPMENT AND STATUS OF SECTION 13, ADP SECURITY

Robert E. Green
Chief, Industrial Security Programs Division, DCAS, DLA

First, some observations about the status of the *Industrial Security Manual* itself. You have been reminded that in 1951 it consisted of 17 pages; today it is close to 400 pages. Why? Two statements may explain. The Industrial Security Program of today is not the Industrial Security Program of 1951. Areas of current concern were not addressed in 1951. For example, international security was not a major problem then. It is now, ADP Security was over the horizon; today it is very much a part of our lives and I will be discussing our approach in some detail. Foreign ownership, control and influence was not *really* a subject of concern at that time, but now?

Quite apart from program changes, the *Industrial Security Manual* has grown as well because of the requests of industry. There has been a constant flood of requests for more information. How do you want us to do it, what do you mean, what are the procedures you would like to see. So, if we reverted to a 17 page industrial security manual, I believe it wouldn't be long before it would be back up to 400 pages.

Now to turn to ADP security. I believe it is useful to describe the evolution of Section 13. There has not been a change in the Industrial Security Program that has had more effect than the final recognition and implementation of ADP Security procedures. Standing alone, ADP systems are one of the most complex and perhaps to the laymen certainly, the least understood advantages of this technological age in which we live.

We recognized, as far back as 1969, that there would be a problem in the processing of classified information in an ADP environment. We issued at that time what are still referred to as the 1969 guidelines. That was the only way they were identified. They were not mandatory; they were simple guidelines. Advice that we tried to provide to contractors to assist them in protecting classified information which they were compelled to use in the computer environment. *Those* guidelines dealt almost exclusively with physical security matters.

Frankly, we didn't know enough about computers then even to address the software problems in ADP systems. It wasn't until 1973 that there was positive movement in the area of ADP security, when a DoD directive and manual were issued for use within the Department of Defense. The directive and manual provided for the first time the concepts of both hardware and software protection. The design of software systems, which would protect classified information, in the computer, and it provided for what was then recognized as perhaps the only two modes of operation that would be necessary. That is the simple dedicated mode when you process batch classified material in and out and go back to operations as normal, or the multi-level mode in which various degrees of information would be processed at the same time. That directive still is in effect.

We started drafting comparable changes and procedures for the *Industrial Security Manual* (ISM) in 1974. It was silent on the area of ADP. The draft largely paralleled the DoD regulations and was sent out for formal coordination. Many of you know that formal coordination in the Industrial Security Program includes some 57 activities. There was a staggering number of comments, good and bad, about that original draft of Section 13 of the security manual, as it later became known. We resolved as many of those early differences as we could, and in 1976, we issued Section 13 of the ISM as a binding contractual obligation. The reaction was both immediate and violent. We literally had some major corporations come to us and say, we will not implement Section 13; we cannot implement it; it is not consistent with the way we use our computer; it is not cost effective.

Well, together with DoD, and some selected representatives of major companies that were in the computer business, we sat down and started immediately to redraft Section 13, to make it more compatible with industry's operations. As a part of that effort, a team, a study group visited a number of small computer outfits as well as some big aerospace industries that had computers that were the size of football fields, in an effort to better understand the problem. A

revision was completed, it was re-coordinated through the same chain, and this time with favorable results. We got indications back from both government and industry that they now believed that section 13 was something that was viable, feasible and that industry could live with it.

I have to qualify that by saying that they agreed with the concept; they certainly didn't agree with the language. The problem then was that it was written by computer-oriented people in the jargon of computer specialists. It was not an easy document to understand. I had my staff undertake a complete editorial revision of section 13. The object was to preserve the concepts and procedures, but to use language that people other than computer specialists could understand. That version has gone to OSD, and I understand that it was approved two weeks ago tomorrow. I have not yet seen the changes but I have been assured that they do not change the concept of the revised section 13.

When we submitted revised section 13, and it had been through coordination, OSD gave us permission to begin to implement it on an interim basis. We had to be able to give contractors using their computers to process classified, some kind of an approval to proceed. So, with that authority to issue interim approvals, our inspectors went out, identifying where computer systems were being used in this mode, examined them against the interim section 13, and if it appeared that that system would qualify under the revised section 13, when it was approved, we gave an interim approval. Now just a few statistics. We have identified nearly 500 systems in industries that are being used to process classified information. Most of those – in the neighborhood of about 300 to 360 or 370 – are operating today under interim approvals. That means that there is a very good likelihood that they will be formally approved when the revised section 13 issues.

Why have we had so much trouble with ADP? And I will admit, and you know, that we have had trouble with it. There are some very good reasons for it. Number one, it was a totally new discipline, introduced into the industrial security program. There was no prototype system that we could go to and say, well how are you doing it; what problems have you experienced, because no one really had faced the problem of security classified information in an ADP system. Secondly, we had to make provision in this whole arena, for any type of system. We weren't dealing with a standard system that you could tear down and look at the nuts and bolts and say, yes, this is it, and this is what we are going to encounter everywhere; therefore, this is the way we will protect it. ADP system engineers tell us, as you probably know from your own operating experience, that there are no two ADP systems which are precisely alike. They are either different in their hardware or their appendages, or they are different in their software. So each one has to be addressed as an individual, specialized system, analyzed that way, and a determination made on a case by case basis that it is a system which can protect classified information, with certain safeguards.

We had no ADP security expertise in the industrial security area to even *address* this problem. I had one man on the staff who was a computer specialist, computer systems analyst as a matter of fact, and a lot of the concepts and procedures that you find in Section 13 were originated by him, and agreed to by OSD. But at the staff specialist level, in the DCAS, we had no ADP expertise, and the Industrial Security Representative on the street was asked to undertake inspection responsibilities in an area for which he had no expertise.

All the documentation for this new element of the program had to be developed. Not only did we have to develop and issue policy in the form of section 13, but also we had to train our staff people and the industrial security representatives. That meant developing courses and then presenting the courses. The Defense Industrial Security Institute had to develop in its programs, training for our people as well as for industry people, in the subject of ADP. And, the local DCASRs education and training specialist had to prepare ongoing ADP programs for our own internal people, the staff specialists and the IS representative.

So we immediately started an education and training for the documentation program. The key ingredient in approving an ADP system in understanding what it is and how it works, remembering that I said no two are alike. We prepared a guide for the preparation of a Systems Description Document or SDD. That document is prepared by a contractor to tell us what his system does, how it operates, what safeguards are built in, whether they are in the manufacturer's software program, or whether they are written into the operating program by the contractor. It is essential that we have the SDD in order to evaluate that system. I am aware that it is not easy to write. Nothing in this ADP area is easy. The guide has flaws in it. I am sure that some of the points can be phrased better and experience and time will see that guide improved, but that was one thing that had to be done.

Then, we had to write some sort of guidance for the staff specialists at the region level who were responsible for approving that SDD – another piece of documentation. Since the systems are not alike, we felt that the IS rep had to be advised by the staff specialist of where the pitfalls were in a particular system. Once he had reviewed an SDD, and approved a system for operating use, the system has to be inspected periodically. We task the staff specialist with developing an inspection guide for that particular system, to point out to the IS rep what he should look for in it and where there are potential trouble spots that need inspection emphasis. So that also was another thing that had to be developed.

Then we initiated a series of continuing ADP workshops for our staff specialists and IS representatives. The purpose is to keep them acquainted with as many changes to the program, as many problems, as many case studies, and as many solutions as we can possibly find to keep them up to speed. Another device we intended to use is an ADP notebook, which will provide, during this learning curve, as much information as we can give to the IS representative, and perhaps even to industry, on our experiences in implementing this facet of the industrial security program.

We are operating under two concepts right now, and I think you will appreciate the fact that they are very valid and very necessary. One is a team concept. We are mixing two disciplines. We are mixing ADP discipline with security discipline. An 080 security inspector, security professional, does not know ADP. An ADP specialist in the government, that is the GS-334 series, does not know security. We don't have the time, and we can't afford the luxury of the extensive cross training that would be required to put both kinds of knowledge in the head of one individual. So we are using a team concept. One ADP specialist, one industrial security specialist, working together for the examination and the approval of systems and the subsequent inspection of those systems.

The second concept we are using, is one that is dictated by resources, and I guess to some extent by just good common sense. We are using a lead region concept; with 500 identified systems, we don't have a full man-year of effort for an ADP specialist in each of our 9 regions. So we have adopted a lead region concept which will provide for the placement of an ADP specialist in each of 5 regions. Those five lead regions will be tasked to provide that service to another region. For example, Philadlephia will service New York. Atlanta will service the Dallas area, St. Louis will service Cleveland and Chicago (Chicago has only two identified systems) Boston is a stand alone, and Los Angeles is a stand alone. As a matter of fact, Mike Craig has been authorized two positions in recognition of the fact that Los Angeles has well over 100 identified systems. We think that is the only way we are going to get the job done, using the team concept and using the lead region concept in today's very tight resource situation.

Now we face the job of converting all of those interim approvals into final approvals. That is, a final examination of that system to determine that it does in fact still meet the requirements of section 13, before we give it that final blessing. We are going to make an advanced distribution of the approved section 13. As you know, it takes months to get a printed change to the *Industrial Security Manual* on the street. We have OSD's permission to make an advanced distribution of that approved section 13 to those contractors who are currently involved with ADP systems processing classified, those that we have identified; as we identify others, we will give them the advanced distribution copy, also. It is an advanced distribution copy only in the sense that you are getting it before it comes out in a manual. It is not a draft for consideration. It is an implementation copy; it is effective when give to you, for implementation.

The advanced change will be distributed through the DCASRs. In the meantime, the Industrial Security Representatives, as a part of their normal, periodic inspections, will be indentifying new systems. Our projection is a 10 percent growth rate per year in new systems. A further projection is that given the nature of ADP systems, there will be a re-approval process following changes to those systems at the rate of about 30 percent growth per year. These are industry estimates based on the changes that they make in equipment and software programs.

So in sum I am saying that we are in an evolutionary period with respect to ADP security. We have brought a program up from absolutely ground zero, concurrently having to write rules, regulations, procedures, and train our people to understand and accept new responsibilities. There are still some areas of concern that are going to be addressed during this evolutionary period. For instance, we are concerned about word processing equipment and other normal business machine equipment which has some memory retention capability. They meet the definition of an ADP system

in that they do have memory, they do process, handle and store information. But it is done in a slightly different environment. We have that problem to face. The second problem we have to face and experience is going to be the rule here, is the onboard weapon system computer. If you are building a missile, and it has a computer, that has a memory, it qualifies under section 13, as a computer system and is subject to its provisions. Some requirements of Section 13 cannot be applied to a weapon system. Obviously we will be addressing that problem as soon as we have sufficient experience and consultation with contractors who face this problem, to be able to address it properly.

The progress in ADP has been painfully slow. We have made mistakes. We will make mistakes again. But with each mistake we learn something, and we are bringing this program, I think, to a point where everyone will recognize it as being an essential, logical and workable aspect of the industrial security program. If there is any consolation for me at least, it came from two different people with whom I spoke at different times. One is a computer expert in the government, the other is a computer and security expert in industry. We had lengthly discussions about the concept of section 13 and what we were trying to do. And in both cases, we were told we are quantum steps ahead of anything that anybody else was doing in the ADP area. Not only in concept, but in our approach to the implementation of the program, and the progress we have made to date. That encourages us to keep going, and all we need from you is a little bit of understanding, a lot of cooperation, and a lot of help. You have given it to us before, and I know you are going to give it to us again. That completes my description of the evolution of section 13.

Now, I should like to touch briefly another aspect. We were pleased to note recognition in this semminar of the field portions of the Executive Director of Industrial Security at DLA. There are three very valuable and essential field extensions of Headquarters. DISCO, of course, is one and you have heard from Mr. Gady. The Office of Industrial Security, Europe, is another and many of you who are involved in international operations, know what kind of a service our office in Brussels provides. As a matter of interest, some studies are underway that may lead to the expansion of the mission of the Office of Industrial Security, Europe – both geographically and functionally.

Many of you are familar with a third extension, Defense Industrial Security Institute, at Richmond, Virginia. We are very proud of the Institute. You may not know that a number of the courses that we present at DISI are accredited by colleges and universities, for undergraduate work in degree programs.

Regarding cost avoidance resulting from education and training is an interesting point. I defy anyone here to identify in specific terms, any costs avoided becuase of proper education and training. The credits that accrue are very real even though they may be immeasurable. If one terminated all industrial security training that government and industry conducts – one could very safely predict a catastrophic rise in loss and compromise as well as all sorts of important but less serious security violations. The nature of E&T follows the nature of the industrial security program itself. Industrial Security is a preventative program and so in education and training. That is why industry has its own internal education and training, and why government does too. That is why DLA has an academic institution that can be used by both. That is why we stress education in our inspections. The IS representative is prepared to give advice and assistance during onsite inspections, and the DCASR E&T specialist is available to assist with programs.

There are eight courses at DISI. I will touch only on the one of most interest to the Society – the Information Security Course. This is not an industrial security course *per se*. We were asked several years ago by OASD to undertake to train government people on the implementation of Executive Order 11652. The concept was to bring classification managers or prospective classification managers of DoD agencies, or those involved in the implementation of classification management programs, to DISI and give them a two week course on how to implement the provisions of the Executive Order and implementing DoD Regulation 5200.1R. The first week of that course is devoted exclusively to the preparation of classification guidance. Some members of the society participated in the pilot test presentation of that course. At the request of the military departments, we have taken that course on the road. It is presented in capsule form in two or three days, where we are able to slant the course more directly to a specific service implementation of the Executive Order and the DoD Regulation. Fifty-six percent of all of the students at DISI during the past year came out of the information security course. This give some idea of the response and the attendance that we are getting in that course. During fiscal '78, there will be 7 resident classes in information security. In addition, there will be 13 field extensions in different parts of the country. The DCASRs will be able to tell

you where and when the course will be held, and make arrangements for attendance.

One of the things that we are contemplating at DISI is the development of some of our courses into correspondence courses. Major corporations do send their people to DISI. They find it cost-effective to send them, but there are some 11,000 cleared facilities and not all of them are major corporations. It may be a one or two person activity, but they need education and training in the industrial security area nonetheless. However, it isn't feasible to participate in our courses in Richmond. We think that if we can do it economically, correspondence courses would be a boon to them. It would be, a boon to us also because the more education they have, the less of a job we have. There is the problem of preparing, distributing and grading papers when they are completed. Also the problem of keeping it updated, so there is a logistics problem which we are trying to work out not.

This completes a brief view of our field extension and particularly the part that our Institute is attempting to play in the industrial security program.

THE BACKLASH OF TESTIMONY

Albert H. Becker
Head, Support Services Division
Georgia Institute of Technology

Summary of Presentation

Mr. Becker who appeared before the House Government Operations Committee, Subcommittee on Government Information and Individual Rights (as it is known now) in August of 1974, gave encouragement to others to do the same.

He was the first member of industry to appear and give views on the security program and a statutory base for it. He noted that his principal intent in speaking was to establish that there *was no backlash.* He commented on the widespread apprehension over the potential loss of contracts. He said that not only did they not lose but rather had gained substantially since the time of his testimony – more than tripling in the case of their DoD Research and Development program.

He said before a DoD Executive Seminar at which he was invited to speak subsequently, "... in my opinion what the Congress does or fails to do for good, or for bad, depends upon how fully they understand the facts of life of security." In urging members of the Society to give their views he noted, "... it is not necessary nor is it required that an industrial contractor obtain the approval of the DoD before giving unclassified testimony regarding security classification procedures before a committee of the Congress. Any industrial contractor who [so] testifies ... is not subject to sanctions ..."

He commented that new laws and their interpretation left the "security forces in shambles, and so weakened that there is serious concern as to whether we can have effective security."

He concluded with the observation that "we must recognize that any system of security based solely on an Executive Order is subject to abuse, and that attempts to enforce sanctions of such a system are doomed in the courts ..." He urged anyone approached to appear and provide information about the system for the good of the country.

PART TWO

SELECTED PAPERS

1978

ANNUAL MEETING – 1978

James A. Buckland
President

NCMS President called the meeting to order.

PRESIDENT BUCKLAND: At this time, we will cover some of our annual business. First I would like to have our Vice-President and Membership Chairman, Dick Butala, give the report on our membership status.

MR. RICHARD G. BUTALA: During the past year we've had a very successful campaign for new members. In May of 1977, just prior to the last seminar, we had 260 regular members, 6 life members and one honorary member, for a total of 267 members in the Society. Since that time until May 8th of this year, a total of 73 new members joined the Society. However, as is always true we lost some members during the year. Nine had to resign for one reason or another or had to retire, and 18 were dropped from the rolls for non-payment of dues. We hope to convince some of them to rejoin.

So for 1978 our new net figures are: 303 regular members, 9 life members, and one honorary member, for a total of 313 as of May 8th. We did finally top 300. That was the goal set last year by then incoming President Buckland. I enjoyed working with him, the whole Board, and the chapter chairmen in reaching this goal.

For information, our Society population is distributed as follows:

	Number	Change
Mid Atlantic	26	+3
Washington	100	+13
Southeast Region	15	-2
West North Central	16	+3
East North Central	77	+1
Dallas	12	+4
South Central Region	5	+3
Southern California	72	+9
Northern California	41	+8

Some other facts of interest. There are 68 women and 245 men, and there are 202 members from industry and 111 from government. The government industry ratio has remained similar at about 2 to 1 for a number of years.

PRESIDENT BUCKLAND: I want to thank Dick Butala for his report and publicly acknowledge that the job he has done in the last two years as membership chairman has been outstanding. He has designed forms and letters, prepared lists, and made many other contributions that will be used for many years to come.

At this time, we will request our current Treasurer, Alan Thompson, to report on our financial posture. Alan . . .

MR. ALAN THOMPSON: This the the third time I've been in front of this group making a presentation on finances. 1977 was a bad year in one sense, but it got us past a couple of humps.

Copies of the year end report for 1977 are available with the area coordinators and the chapter chairmen, and you may examine it in detail when time permits and pose questions later. Of course, I'll entertain questions as I complete this report. We opened calendar year 1977 with a net worth of $14,370. We ended the year with a net worth of $9,770 for decrease in the net worth of the Society of $4,599. There were a number of good reasons for this and consequently the change was not a surprise. Some of the reasons are of interest.

First of all, we published three journals. Each of them cost approximately $2,500 to make up and distribute. Net cost of the journals was something like $7,636. Last year we published seven issues of the *Bulletin.* A number of those issues carried extra pages, which meant increased cost not only in printing but in postage.

Also we reprinted the bylaws of the Society, membership applications and brochures for a cost of $882. So, the bottom line was a net worth at the end of the year of $9,770.60.

Your Board recognized as we came near the close of last year that it was necessary to increase dues and the initiation fee in order to assure ourselves of income sufficient to meet ongoing expenses for 1978.

During the year our President appointed a Finance Committee to examine the accounts of the Society and to submit recommendations. The Committee was comprised of past Society presidents Gene Suto, Jack Robinson and Jim Bagley. We met and spent a good number of hours going over our account structure. Some feeling existed that our very rudimentary accounting system needed additional structure to describe better and define more precisely where various categories of expenses ought to be included. The goal was to present the information about expenses in such a way that it could be considered. Difficulties had existed in being able to find easily, for example, *exactly* how much we were spending on the *Journal.* This then led to problems in planning a budget.

The recommendations resulted in changes that are reflected in the 1978 budget as it was prepared. As an incident to these considerations and recommendations, I was personally pleased that they determined also that the accounts I had been keeping for some three years were in good order!

Turning to the present. We are approaching the mid-point of 1978. Because we took the painful step

of increasing dues, together with the increased membership resulting from the success of our Vice President/Membership chairman Dick Butala, we are in a fairly reasonable state. As different from the 48 dollars in the checking account on 1 January there is some $2,000 plus. Some $7,000 in dues and initiation fees have been received and some put into Certificates of Deposit of varying lengths and a savings account. We retain enough to cover expected payments but not more.

That concludes my oral report, Mr. President. I remind that the full details are available in a written report available through the chapters and area co-ordinators.

PRESIDENT BUCKLAND: Thank you Alan. A time comes – and I think it happened to me about 3 or 4 weeks ago – that one gets the lame duck feeling. Now it feels real good. I want to thank again the Board, the Chapter Chairmen, and all the individuals whom I have called on. Your support has been fantastic. I would like to summarize now, some of the highlights of the past year.

- We achieved our goal of 300 members plus and the Board of Directors has approved the addition of two new Directors to the Board, effective with our Annual Meeting next year providing we still have 300 members as of 31 Dec 1978.
- We achieved a major goal on 31 December 1977. At that time all of our publications were current and delivered, and we had no outstanding bills. This enabled us to start this calendar year with a clean unencumbered new budget.
- A note of disappointment – our essay contest was totally unsuccessful. We had no entries.
- We held no mini-seminars during the year. However, that is understandable because all of us have been waiting for the new Executive Order and the new DD Form 254. However, I believe that the time the Board of Directors and the Society spent on the preparation and development of the new Executive Order, more than compensated for the seminars.
- We have increased our liaison with ASIS and other Security groups. We made a presentation jointly with DLA at the 1977 ASIS Seminar, and are planning to conduct a workshop at their 1978 Seminar.
- We have established new committees for finance, editorial review, and records retention. Read about these in the next *Bulletin.* We are trying to establish a new operational basis for the future.
- As a last but not least note, we have a firm commitment from the Northern California Chapter to hold the 15th Annual Seminar in San Francisco, California in May of 1979. Be there.

Looking forward, I am pleased to announce the three members elected to fill vacancies on the Board of Directors. They are:

Frank Larsen
Alan Thompson
Marilyn Griffin

As my last official duty I am pleased to present your incoming president who will conclude the meeting, Alan Thompson.

INCOMING PRESIDENT THOMPSON: I want to make a comment first that Jim Buckland has done a fantastic job this past year. I have been on the Board only three years but I want especially to commend him for his accomplishments during this last year. I'd like to touch on some of the aspects. He provided that strong and steady kind of leadership that is needed at the head of our professional organization. It made it possible for us to move and to change in a time of change.

Some other specific points: *Bulletin* has become a vital, *current* medium for getting the word out on what is going on in our business, and what it is that we should be paying attention to. He has improved the management of the society in the appointing of the finance committee which I reported. We re-structured our accounts to enable logical consideration of budgeting and financing. He has made better, more direct communications happen between the top of the society, and the chapters and area coordinators. He has made himself available to meet and has met with chapters, and that has helped improve exchange. Finally, he has left me with a new legacy, something that will help me and will be available to my successors through the years, and that is the President's Advisory Council. It is comprised of past presidents, with the immediate past president chairing the group. It is to that group that I will be looking for assistance, direction, guidance, and good counsel. I know you join me in expressing our sincere appreciation for Jim Buckland's leadership during the past year.

As incoming President it is desirable to set forth, albeit seemingly more modest than those established similarly a year ago, the program views. If there are to be goals, let them be four in number:

First – Maintain and strengthen that direct liaison which we have established, particularly during this past year, with the Executive Departments and Committees of Congress. We must stand ready to provide the very best possible advice to express to those people, the professional concerns of you the members of this profession as it develops further.

Second – Take every action that is required and possible to assist the members of the Society in the performance of all of their functions. I personally pledge my assistance, I know the Board is behind me in this regard. To do that, we need to know what are your concerns, and we will be exploring in our board meetings and in our personal way, how we can make that happen.

Third – Promote, in every way we can, mini-seminars and educational opportunities. It is especially important that all of you join me in supporting most particularly, the seminar next year in San Francisco. They have got a good start on it, they know where they are going, there is fine leadership there, and at the same time I am sure they will appreciate any and all assistance that you can give.

Fourth – Increase the membership of this society further. There are a great many people of whom each one of us is aware who are now and will be increasingly coming into responsibilities in this field, who are not active members of this society.

I appeal to you and invite you to join me in making this an active viable, vibrant society for next year and the future. In conclusion, it is my pleasure to present the other elected officers for the coming year. Thank you.

Vice President	Frederick Daigle
Secretary	Marilyn Griffin
Treasurer	Jack Robinson

CLASSIFICATION, CONTRACTS, AND COSTS[1]

Frederick J. Daigle
Lockheed Missiles and Space Company

INTRODUCTION

At the outset of this paper I have two premises:

- **SECURITY COSTS ARE BEING PREDETERMINED WITHOUT CONSCIOUS KNOWLEDGE OR PARTICIPATION OF THE SECURITY MANAGER**
- **COST *SAVINGS* IN SECURITY IS NOTHING MORE THAN CORRECTING A SITUATION THE SECURITY MANAGER HAS DIRECTLY OR INDIRECTLY PERMITTED TO BE CREATED**

A Security Manager likely is ready to take offense at both premises. They are meant to be offensive. They are meant also to cause question about the audacity of the writer and the basis on which he could make such statements. I believe I can justify the premises and in turn help rectify, at least in part, the actions that I feel are the basis for such premises.

[1] Presentation before the 24th Annual ASIS Seminar, September 1978.

Clearly, we are addressing those in the field of security classified government contracts, otherwise there would be no authority to have classified information in our possession, and no reason to proceed any further on the premises. However, *CONTRACTS* and their protection are critical to the Information Security Program.

THE CONTRACT SEARCH PROCESS

It is my position that no business should attempt to enter into any contract with the government involving access to classified information without a qualified classification manager on their team. Let's follow the involved trail in getting these contracts and you will understand why. Your marketing group faithfully reads the *Commerce Daily* to see what tasks the Government is putting out for bid. When an item of interest appears, the first positive action – after the decision to pursue the business – is the Procurement Qualification Letter or Qualification Package, where the marketeers do their utmost to prove to the procuring agency that

they are, in fact, fully qualified to bid. Although not a cost avoidance problem at this point, definitely a security problem – what have they volunteered that may be classified or politically unwise? Does the CM REP participate in the marketing evolution? And does he have final review/refusal authority for security classification matters? Next comes the real problem, THE RFP.

The joy of marketeers in receiving an RFP is second only to the joy of winning the contract. Receipt of the RFP sets in motion a whole string of activities, each of which is supposedly coordinated, but often times autonomous and anonymous – the most anonymous of which usually is the classification/security loop. Your company now has to prepare a proposal. This can range from a simple cost estimate to a full blown multi-volume detail plan of how you can do the job better and perhaps more economically than your competitors. *Proposal* teams are the lifeblood of industry and government. However, they can, if not properly supervised as to classification and security commitments, become your worst enemy.

When the RFP is received, a complete review is necessary, not just of the Classification Specification, the DD254 and the guidance attached to it, but also the work statement and the technical requirements volumes. Be aware, the classification intent of the customer is more often revealed by his actual paragraph marking of the work statement and technical volumes than by the words in the classification guidance. Any **DIFFERENCES MUST BE RESOLVED** using the procedure specified in the RFP. If this procedure is not effective and you can't resolve the differences, then you and your management should discuss and include in the RFP response (the proposal), a strong position for revision of the guidance you consider to be in error, inconsistent, or financially unsound. *Write* a revision to the provided guidance with a rationale for your changes and include an appropriately reconstructed DD254 or better yet, prepare a security risk analysis for the customer's consideration. A security risk analysis is a trade-off between protection, attendant schedule delays, and fragmentation of information *vs.* cost and state-of-the-art. This shows security awareness, is the purest and most effective form of **COST AVOIDANCE**, and, at the same time, is the most constructive way to enhance security classification guidance.

READ ALL OF THE

RFP OR CONTRACT

NOT

JUST THE 254

Many companies today are involved in critical sensitive defense work and many in some type of "carve out" activity. It may be a simple Special Access Required (SAR), or it may be a complicated Communication Security (COMSEC) contract, or it may involve Sensitive Compartmented Intelligence (SCI). Whatever, it is part of your product line, part of your capability, and one of the things your writers tend to use to prove the capabilities of the company to do exotic work. It is also a potential booby trap for compromises and for hidden costs.

I mentioned the *Commerce Daily* in connection with how an RFP may be obtained. There is of course another method of receiving an RFP; the personal contact by the technical marketeers and the user agencies. Companies all spend great sums of monies to foster this type of relationship. It brings us closer together and we understand better each other's needs and capabilities. *But,* what has your technical marketeer said to assure the potential customer about the company's ability to provide additional security should added sensitivity be assigned? There have been instances of assurance that certain security-approved facilities can be used when they are already otherwise committed or do not in fact currently exist. Also, that certain specially briefed people are available who are possibly otherwise committed or whose briefings are not transferrable because of billet limitations. How are you, the security manager, going to cope with providing these security capabilities unless you *know* and *budget* for these committments, should the RFP be successful?

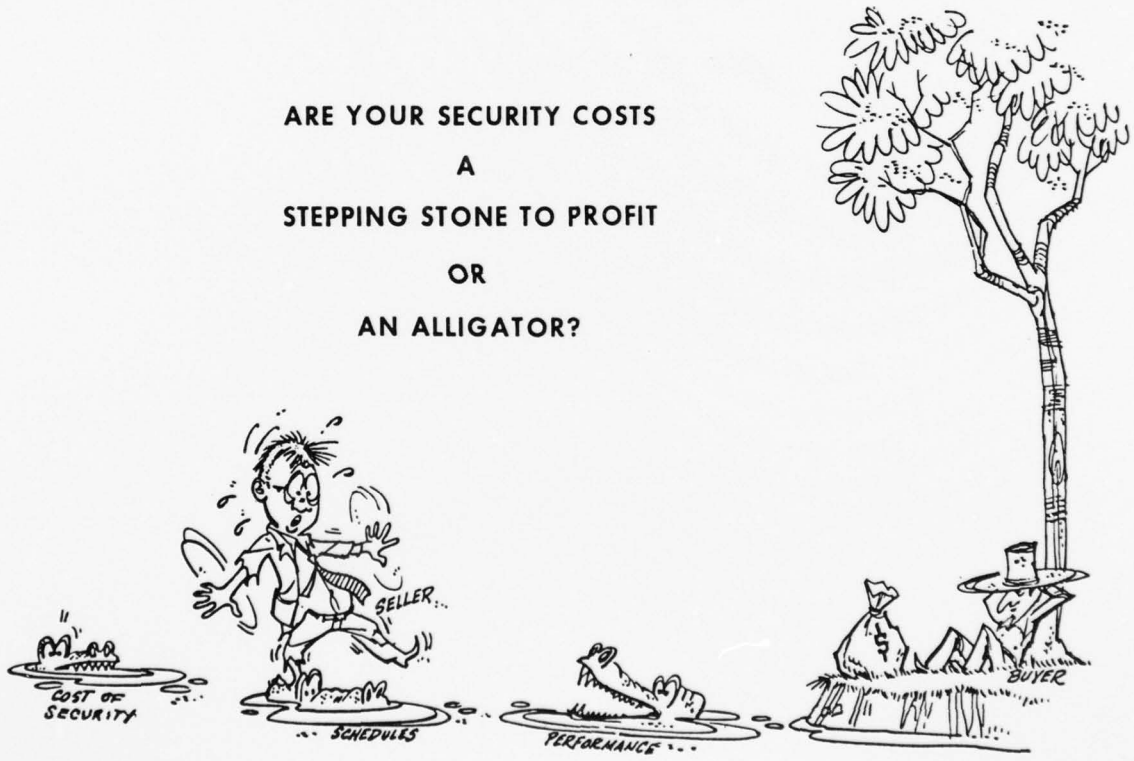
ARE YOUR SECURITY COSTS

A

STEPPING STONE TO PROFIT

OR

AN ALLIGATOR?



In any company, and especially in large companies with splintered groups working varied technologies, the only way you can assure yourself of such oversight is to have your company procedures include Classification Management as a member of each proposal team and insist that it have the last possible review prior to final printing because we all know that every reviewer in the chain of command can and may add his own touch – Classification should finally review all such changes no matter how trivial they may seem to the

ENSURE FINAL REVIEW BY CLASSIFICATION MANAGEMENT

harried proposal leader who has two hours left to print and ship. *OK,* so your CM rep does get some 2:00 a.m. assignments – the rewards to you will be worth it. This, of course, pre-supposes that the CM rep has been instructed and trained, to look not only for proper classification and marking of the written words, figures and illustrations, but also at the security committments and implications, as well as to consider the political nuances. Provide for careful, thorough review. Sloppy security in handling of the proposal documentation, could be considered a signature forecasting sloppy security under contract. The Security or Classification Manager must **GET INVOLVED IN PROPOSAL ACTIVITY!** I submit that my premise, your security costs are being predetermined without your prior knowledge or participation, is supported if the necessary steps I have described have not been followed. The next phase of our little drama is called:

CONTRACT!!! WHAT NOW?

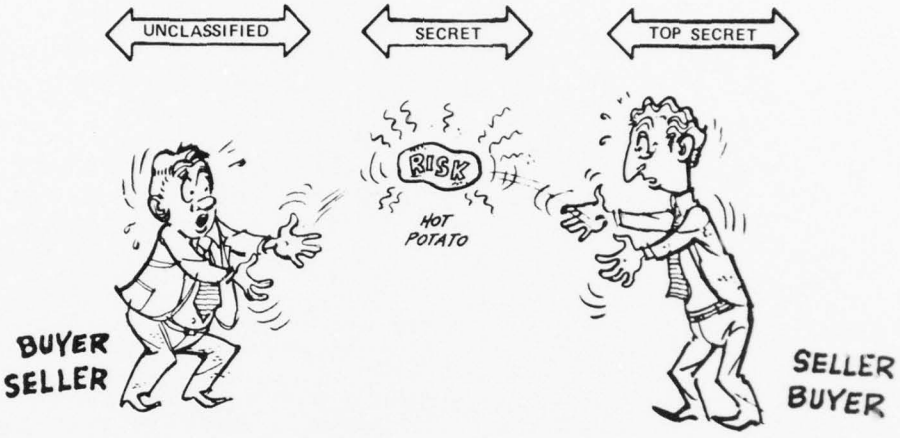
It may seem like I'm belittling the technical types; it is *not* belittling but everything I say is based on fact and experience. When you win a contract, the first thing, you the Security Manager, should ask is, *"what verbal promises were made after the RFP went in?"* Did *you,* the security manager, have the oral presentation reviewed before *they,* the technical team, left for the customer's facility? Most proposal cycles include "Orals" – orals are a short stand-up review of a voluminous proposal and are subject to questions. The floor questions answered with commitments you did not know about – DID YOU DEBRIEF THE TEAM AFTER THE ORALS?

The time between notification of a WIN and receipt of written contractual documentation can be extensive, you can be comfortable if you have done all the good things I have mentioned, or unrestful wondering HOW HAS THE COMPLEXION OF THE CONTRACT CHANGED SINCE THE RFP? IT DOES – QUITE OFTEN. I just recently received a contract package on a win proposal that was followed through in classic style, and to my chagrin, the Classification Specification for the first time authorized access to Sensitive Compartmented Information – a subject never addressed in the RFP or the proposal. But, the technical director in the customer's shop threw it in at the last minute with our Study Manager's concurrence because *"He (the customer) thought we might be able to enhance the proposal through such an access."* When asked about access billets, stated *"Oh you guys have briefed people out there".* Both these statements are true. However, to have custody of SCI material you need a special closed area – ours were all occupied; you need special briefings, our people with those briefings were all committed on other projects.

The Security Manager was immediately in the middle, to provide a new area, and process more access requests. How did I, the Classification Manager handle it? As the designated company single point-of-contact for classification matters, I visited the customer – because I was technically knowledgeable on the project – convinced him that that special access was in fact not required – or even authorized through proper channels – and eventually got the requirement deleted along with the attendant costs. This was a cost avoidance that we thought we had covered in the RFP stage; it *could* have developed into a downstream cost savings – after we started to build a new area, for example. However it was an avoidance because as it was sidetracked prior to commitment of funds. BELIEVE ME – YOU CAN GET TRAPPED.

Returning to the contract, immediately upon receipt review the Classification Specifications to ensure there

—A FUNCTION OF RISK



are no changes or surprises. Even more important, now is the time to review (with the technical people):

- Contract Statement of Work
- Contract Data Requirements List (CDRL), DD Form 1423 – Section 5 in particular
- Special terms and conditions – In this section security requirements are usually amplified – and special requirements imposed
- Performance and design requirements – it should be paragraph classified. Is there a difference in their classification from that required by the contract – if so find out why and correct one or the other
- *Management system summary list – DD 1660* (Item 2).

In addition be aware that some agencies do indeed direct contractors to classify and mark over and above the requirements of the Industrial Security Manual – and do not always so indicate in Section 10. c. of the new DD254 (1978). Some of these could be:

Defense Nuclear Agency – They require compliance with STANDARDS FOR DNA SCIENTIFIC AND TECHNICAL REPORTS

U.S. Navy – Often requires page markings more severe than the ISM

Intelligence Agencies – In addition to SCI requirements they often impose additional other requirements

Special Access – Many variations are imposed, some very severe and very expensive.

If your company's policy is to charge direct to the contract for excessive security requirements, you should know of these excessive security markings as well and determine if you desire to challenge and charge. The message here is KNOW YOUR CONTRACT. Do not rely on the contracts organization or the technical people to analyze it for you. You may discover too late that you are obliged to provide *security requirements you did not budget for, but the* program manager "Knew it all the time – thought you did too!"

CONTRACT OPERATIONS

So we have accepted the contract and now are proceeding to get ready to build the system the government wants. Do you track the progression of the contract to ensure there are no changes or surprises – like your Responsible Engineer for the Communication System who knew all along that company Blue made a

specific component and how much they charged based on careful history review. He priced the item at the cost. Now, unbeknownst to him, the customer had directed that the RF frequency for the component, when purchased for this project, must be protected as classified, and your engineer finds that company Blue has no facility clearance, no closed areas, no briefed people. What do you, Mr. Security Manager, do now? Let your company pay the bill for such capability? Get the requirement modified by the customer because you did not foresee this during the RFP stage? Change suppliers and get a contract modification to that effect? *WHAT?*

By way of a few further thoughts regarding engineers, let me quote you from a presentation made to the Northern California Chapter NCMS meeting in September 1977 by Mr. Don Ricketts, a senior engineer with GTE Sylvania.

> "When we talk about the engineer's interaction or knowledge of the Contract Security Classification Specification, we are really talking about a person who is interfacing with information. When that happens, there are three basic ingredients to complete interaction and knowledge. That is, if you are going to impart knowledge, you have to have (1) a desire to know; (2) an ability to understand; and (3) available useful information. Let me amplify upon these three major components or links of imparting knowledge. When we talk about the desire to know, we really have to look at the nature of the engineer. Does he really have a *desire* to become knowledgeable? In general, the answer is yes; engineers are very inquisitive people. However, engineers typically prefer to excel in technical areas, and do not like to learn administrative or management matters. He typically does not like cost responsibilities, schedules, writing or security procedures. It is the non-technical demands that he sees as impediments to his ability to technically excel. Getting that extra dB of gain from an amplifier or triggering an oscilloscope to a 30-nanosecond pulse is far more rewarding than classifying a report properly, or safeguarding a document properly, or even being on schedule. The exception is, of course, when his yearly salary review comes due and he gets a minimum 3 percent increase. Then he realizes that his high technical performance did not offset his late delivery, or his overrun, or numerous security violations. So, one part of the chain which allows an engineer to interact with the DD Form 254, namely his desire to know, is not complete. His desire to know is not high, and this is one of the impediments in allowing a good interaction and a good knowledge of the DD Form 254 in the engineer's world."

—COST SAVINGS IN SECURITY

IS NOTHING BUT A CORRECTION OF A SITUATION

YOU THE SECURITY MANAGER HAVE DIRECTLY OR INDIRECTLY

PERMITTED TO BE CREATED

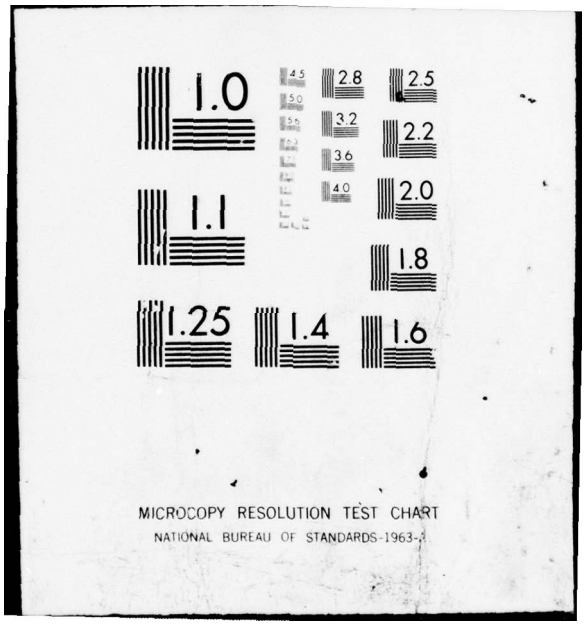
IS IT OR ISN'T IT ?

AD-A068 235 NATIONAL CLASSIFICATION MANAGEMENT SOCIETY ALEXANDRIA VA F/G 5/2
CLASSIFICATION MANAGEMENT. JOURNAL. VOLUME XIV, 1978,(U)
1978 J A ROBINSON

UNCLASSIFIED NL

2 OF 2
AD
A068235

END
DATE
FILMED
6-79
DDC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Your *classification* representative should maintain constant liaison with the customer persons responsible for classification – I wish I could say the CM rep of the customer in each instance. However, too many customers have not developed this capability. Frequently their technical people dictate the classification requirements. One hopes this will change, but in the meantime – you must maintain contact with whomever has the responsibility.

I believe I have substantiated my second premise: and rest my case.

THE CASE FOR SPECIAL ACCESS PROGRAMS

Maynard C. Anderson
Office of the Chief of Naval Operations

INTRODUCTION

"If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed, and in the next place, oblige it to control itself. A dependence on the people is, no doubt, the primary control of the government, but experience has taught mankind the necessity of auxiliary precautions."

So it was written in *The Federalist,* No. 51, at a time when our forefathers sought to establish a place in which they could live as they wished. Those perceptive words are wisdom even now. Dependence on people is a primary consideration for all of us and surely for all of us in professional security endeavors. If an individual is so inclined; neither high walls, vaulted doors, nor sophisticated locks will prevent him from taking out what he wishes to share with someone else. The auxiliary precautions referred to by Madison and Jefferson were, of course, those to be included in the machinery of a new government.

The need for precautions and security is not new, as you know. Some 200 years earlier, for example, it was unfortunate that Magellan couldn't stay his full term in the Phillipines because somebody stole his anchor. He then realized the value of intelligence and security as he properly concluded that a member of his staff should have guarded the anchor; someone should have given a warning; someone should have found the culprit. He *should* have had a professional security officer! (Parenthetically, an intelligence assessment of the probable state of mind of the natives on Cebu might have provided the information to plan differently and thus avoid his untimely demise – at their hands.)

However, in the almost 200 years since Madison and Jefferson wrestled with the concept, the evolution of auxiliary protection devices would surprise even those astute men. As professionals in this field, you recognize that evolution and what it takes to accomplish your mission today. What is needed from a professional? Probably the foremost assets which we must demand are personal integrity and that discipline of self which instructs a man or woman in the knowledge of the craft. Both require dedication and a grueling work schedule. But, it is the way to learn how to achieve the excellence that is the mark of the professional and what criteria are used to measure achievement. Such criteria and they differ among the various fields – we must attempt to apply to our daily work to serve a modern day defense establishment as it contends for parity in a bi-polar world; and concurrently to serve the information needs of the customers in the establishment as well as the public for which that establishment exists.

We seem to be always in some state of crisis in this security arena as we struggle to protect information determined to be *sensitive* and yet ensure that information gets to all who *need to know.* The commitments of this two fold mission inevitably produce tension. But, I submit that the tension is creative and conducive to producing the proper result. There is always tugging and pulling from both sides.

To dramatize the case, on the one hand program managers are prone to insisting that *everything* relating to their program must be protected from disclosure or the national defense will go down the drain. On the other hand, seemingly competent authorities are saying that this same information must be released to seemingly vast numbers of people who have a legal or regulatory right to know apparently the smallest details – auditors, contractors, Congressmen, investigators, inspectors, *et alia* – or the program will never "get off the ground."

THE GOALS OF ACCESS CONTROL

Having established a background for the arena of conflict, albeit briefly, how does one resolve the seemingly irresolvable? One must ensure by whatever means that only *essential* information is protected. One must also ensure concurrently that those who have a *need* to know – whether Congress, contractors, analysts, scientists, or whomever – can learn what is afoot *and* be obliged to protect sensitive information. That is the framework on which we hang the fabric of all information security management. Special Access programs have no different goal. They:

- Protect essential sensitive information; and,
- Ensure dissemination to those who need to know

And that is the whole cloth from which is cut the pieces of all security management:

- Personnel security
- Physical security

- Information control.

These so-called special access or compartmented programs are sometimes regarded as untouchable. Surrounded by mystery, they sometimes even create fear in the uninitiated. But, we are well advised when encountering these programs to ensure that we do not become so bound by tradition, so trapped by the past that we react over-defensively. Undue caution and reluctance to risk change will accomplish nothing.

There are new and different challenges every day to many of our programs. You are aware that there is a vast effort by potential adversaries – both overt and covert – to obtain information. However, there is also the problem of the lack of legal status for protecting most programs and the action of the courts in judging whether an individual is bound by a security agreement. A loss of information through espionage has no worse effect than a loss through the judicial process, or inadvertence.

However, must a special access program be established to exist in perpetuity? Of course not. Only as long as necessary. Threats and challenges are dynamic and so must be program management. This is not to say that the task is easy. In our system, balancing the principles of openness and secrecy in the face of the challenges and frequently incomplete knowledge of the whole picture is difficult indeed! How does one try to improve the outcome?

First, inappropriate definitions, and terms unsuited to the program or purpose must be recognized as a threat to success – incidentally applicable also to any organization, group, or function. When inappropriate definitions are applied, equally inappropriate results are likely to follow. For example, security officers are, as a group, often considered obstructionists; labeled as negativists and regarded by many as an obstacle on the road to mission accomplishment. The genesis of the problem may well be the failure to have defined correctly, in the first instance, what was intended.

Second, what about our own general approach and current personal reactions? When presented with a request, do we quote "the book" and close the door? Are we the commander's *advisor* on security matters? Or, are we only the keepers of the keys to the information warehouse?

These two factors apply also in the case of special access programs – about which erroneous conclusions are often drawn. It is a field, however, in which a little knowledge or a total lack of knowledge is truly dangerous. Let me illustrate by anecdote and quotation:

Three men were sitting in a boat fishing about 50 feet from shore. They were drinking beer and it was a warm afternoon. One of them got up, walked to the shore without getting wet, went to the bathroom and returned to the boat in the same manner. After a few minutes, the second man followed the first accomplishing the same end. The third fellow thought a bit and decided to follow. He stepped out of the boat and immediately sank into the water up to his armpits. The first guy looked up and said to the second, "Hey Charlie, should we tell him where the stones are?"

Benjamin Franklin is quoted as having said that three may keep a secret – if two of them are dead.

The story of the fishermen and Franklin's quote illustrate both the consequences of protection of information and the importance of its dissemination. Two of the fishermen were, you might say, privy to a special access program while the third remained "outside the door."

We must continuously ask whether it is time for a change. There is within any system always need for a vigorous and articulate defense of what has been accomplished balanced against a recognition of the need for progressive and beneficial change. What can we say about the achieving of goals?

PROBLEMS IN ACHIEVING THE GOALS

It is true that bureaucracies are alleged to be prisoners of yesterday's policy positions. However, the intelligence community is currently considering whether all present systems of security are appropriate and effective or whether there might be some alternate systems or methods to accomplish the goals. In these deliberations, there are some basic questions that must be asked:

- Do the existing systems – as used by each of the members of the intelligence community, for instance – provide adequate security?
- Are the systems effective in providing for necessary dissemination of information?
- Have the systems become so large, so well known, so accepted that effectiveness has been diminished?
- Do we have a security problem? A dissemination problem? An education problem? Or a general management problem combining all of these factors?

I commit these questions to you also for consideration along with some observations of the status of what one might term the intelligence program.

We have a system or systems – and I use the term generically – designed to provide protection to information which, if disclosed, may impact severely on the national security of the United States. Now everyone can think of examples in which we have used the system in a way analogous to putting bandaids on fractures and splints on ulcers.

The concept of need to know has been ignored. The rubber stamp syndrome has at times overtaken us and for the sake of convenience, or foolishness, or laziness, information of not the slightest substance has gone into the secret safe. On the other hand, the intelligence community of the United States has some of the best informed safes in the world – one must admit, sometimes to the detriment of the operating forces!

Our systems originally functioned within the boundaries of need but often they seem now to have lost their utility. The original concept insured that sensitive material was known to a limited number of people with an indisputable need to know. Now there are increasing demands for more secure, timely, less costly processing and dissemination from new, sophisticated, high volume collectors of intelligence.

As consequences, access proliferation and information diffusion cause extraordinary concerns as to whether need to know still exists or it merely continues to receive homage out of respect for the memory. Because of this and claims of necessity, systems have added to systems. The assumption has been that the systems provided security to new programs. It might be speculated that, at times, access to the systems is little more than the key to an inner sanctum. Indoctrination into their rituals has been established as the *sine qua non* of prestige.

It has been concluded by some that restrictive and outmoded security policies are an impediment to improvement of the quality, scope and timeliness of intelligence and to achieving a more efficient use of resources involved in the handling of information. That conclusion has been drawn by officials within the intelligence community as well as by consumers of the product. The real issue to be resolved in application of any sort of security control is *Risk vs. Utility.*

A continuing assessment of the threat to a program – its development, its use and its product – is essential to determine application of security resources. If information is compromised in the RDT&E stage of a project, the possibility of damage is often greater than during the fabrication process. Therefore, the threat of real damage may lessen with each stage of advancement. On the other hand, there will be programs in which there may not be a significant threat until all of the pieces have been put together and a sensitive mosaic then emerges. The lesson, then, is that threat assessment must be dynamic and it must be an integral part of classification management in every kind of program.

You know there is risk in every situation and the key to handling it is how we respond. If the threat to sensitive information is communicated to the classification authorities for the information in a timely manner, the necessary decisions concerning classification designation, downgrading and declassification, as well as access can be made.

Advancing technology – namely, a constantly changing "State of the Art" – presents formidable problems. There is probably no way in today's world by which all necessary data can get to all who need it quickly. The scientists, the research specialist, the program manager all face the same dilemma as the security officer: How to keep up with an increasingly dense flow of significant data and apply it appropriately to the project at hand.

To illustrate, a century ago, it may have been possible for a truly well educated person to absorb almost all of the knowledge of importance that had been accumulated by mankind. Today, human knowledge is expanding so rapidly that no one can catch up with it. Robert Hilliard, Chief of Educational Broadcasting at the Federal Communications Commission, says,

> "By the time the child born today graduates from college the amount of knowledge will be four times as great. By the time that same child is 50, it will be 32 times as great and 97 percent of everything known in the world will have been learned since that child was born."

However, the memorizing of reams of facts will not be necessary. They will be quickly available in computers. But future man will need great knowledge if only to know what it is he wants to know. The 1976 publication, *Future Shock,* by Alvin Toffler, created an awareness about the burgeoning and almost uncontrolled growth in technology. For instance:

- We find that by the time a new electronic item is in the field, its key components may already be out of production

- Scientists and technologists dare not wait for their current journals. They must study preprints of articles and use the telephone to be sure their work has not been made obsolete by what someone else did this morning.

From an information security standpoint, there are fascinating facets to this situation. The splitting of the atom and exploring of space bear witness to the stimulus of competition and illustrate the convergence of interests; resulting in accidental collaboration with potential adversaries. Technology is the natural foe of nationalism. There is a sense of cooperative accomplishment among the "Republic of Technologists" – regardless of national loyalty – as they solve the problems of military application as well as general use of technology. It is difficult to prevent cross-talk in this situation. Information of technological or proprietary advantage to the United States, even if not of security significance, is often revealed in an atmosphere of mutual interests.

Implicit in this scenario may be one of the best arguments in support of compartmented programs; we need to attempt to preserve whatever informational advantage the United States may have, and at least make it more difficult for other nations to collect information of real strategic value. On the other hand, perhaps it's the opposite. What we *do* to assist in protection must be considered and whether what we do is effective must be assessed.

The basic ingredients of the program are straightforward. "Compartmentation" or special access does not differ substantially from any other program that provides protection, it merely:

- Establishes somewhat more extensive requirements for investigation
- Reminds program managers, subordinates and superiors alike that a determination has been made to severely limit access and dissemination
- Establishes Access Lists to reflect determinations on who and which *really* need to know
- Prescribes protection measures somewhat more stringent than those for other information or material.

One must recognize that such measures cost money and require people (another aspect of money). What with the emphasis on reducing – both in people and other resources – costs, questions arise. Is the expensive administration in the form of investigations, maintenance of access rosters, and ensuring physical security, cost effective? How much security do we get for our dollar? Does the program guarantee no "bad apples?" The answer to the last question is, of course, no. The answer to the first and second is a problem. Effectiveness with economy is the new order of things. I am reminded of something I once read (although I have forgotten the author) which speaks to both the threat and our efficiency:

> "So long as the bureaucracy consists of large numbers of people at many levels who believe they perform their functions of evaluation and approval properly by requiring vast and detailed information to be submitted through the many levels of the bureaucracy, program managers will never be found who can effectively manage their jobs. A program manager today would require at least 48 hours a day of his own time just to satisfy the request for detailed information from the Bureaucracies; The Congress, the General Accounting Office, and various other parties who have the legal right – and use it – to place demands on their time. As long as we operate a system where the checkers outnumber the doers (those responsible for carrying out the work), the doers are condemned to spend their time doing paper work for the checkers."

So, security administration is inescapable, but security *management* is indispensable. The utility of any program's product cannot be determined until it gets to its ultimate consumer. Our constant objective in the compartmented world is to get that product out within acceptable risks. It is recognized that with each system modification, new evaluations must be made. There is a foundation of experience in terms of unauthorized disclosure of classified information; in terms of clearability of personnel; in terms of the likelihood that an individual will commit espionage. The problem of the unpredictable, as noted earlier, or the outcome in the absence of the special effort, is difficult to weigh in a statistical formulation. However, if any system is professionally employed; if the professionals charged with responsibility for its employment contribute to its improvement; if those for whom it is designed as an information control system are properly served; and, if the goals of protecting an advantage of the United States are achieved, the systems detractors will be denied a valid basis for their complaints.

FACTORS FOR CHANGE

To restate, basic United States policy is to limit access to classified information on a "need-to-know" basis. I suspect that the first special access program, in a modern context, was developed because it was concluded that the principle of need-to-know was no longer effective. One may observe that if the principle was properly implemented, formal special access programs would have no basis for existence. "Need-to-know" and "Special Access Program" are not mutually exclusive terms. So special access programs exist in the belief that formally restricted access procedures will succeed in restricting the dissemination and availability

of information. Some factors have come on the scene that probably will affect the program as we have known it.

The first factor, now not new, that undoubtedly caused the effect of increasing the number of programs, was the Freedom of Information Act of 1967, augmented by the changes of 1974. Then, relatively recently the President signed EO 12036, "United States Intelligence Activities," that formalizes in greater detail the responsibilities, authorities, and limitations on the several components of the intelligence community. It recognizes – by assignment of certain responsibilities – the need for compartmented programs. That recognition would be carried forth in the charter legislation now being considered by the Congress (Senate bill S2525 refers).

The proposed replacement to E.O. 11652 also will impose some new requirements. If signed in its present form (winter, 1977/78), it will require that all compartmented programs be justified within 180 days of the Order's effective date and every three years thereafter. Thus, the need for such security measures as compartmentation is recognized but their proliferation without justification will be controlled. *(Ed. note: E.O. 12065 was signed on 28 July 1978 and provided a five-year terminal or rejustification period rather than the proposed three-years)*

Such policy is welcome because, in an arena such as this, a multiplicity of programs all with different requirements is a mangement burden. There is an old Irish adage perhaps applicable: "If you don't know where you're going, any road will get you there." There is hope that the new approach along with some other initiatives underway will put us on the one right road. What we must avoid is that limitation endemic to all efforts aimed at statements of general policy which is that they frequently do not and can not provide clear guidance for responses to particular events unknown and unanticipated when the policy document was written.

I think special access programs do diminish the vagueness and generality of some policy documents in that they impose specific criteria for administration. They put particular issues into focus while still allowing considerable flexibility in decision and action if properly implemented. And, of course, they allow the ability to:

- Assure data privacy
- Eliminate superfluous information
- Strengthen disclosure control by giving real meaning to need-to-know
- Enhance storage and transmission security

On 31 December 1974, President Ford signed Public Law 93-579, better known as the Privacy Act of 1974. In enacting the law, Congress was concerned over the encroachment of new technology on the individual. Concerns over the impact of technological advancement are not new – as early as 1890 the Harvard Law Review published an article about instantaneous photographs and newspaper enterprises as having invaded the sacred precincts of private and domestic life. If one accepts the definition of Alan Westin in *Privacy and Freedom* (New York: Atheneum, 1967), to wit: "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others, " then it would seem that the government also has a right to institutional privacy and the obligation to protect, on behalf of its citizenry, that information essential to the national security. In so doing, if it is necessary to restrict access to certain information by some formal administrative means to preclude damage to the citizenry as a body because of unauthorized disclosures, then it would seem only appropriate to establish a compartmented programs system.

Let us not believe, however, that these "auxiliary protective systems" are such that we can rest easy. It has been written that no age in history can afford to lay too much emphasis upon security and we must recognize that it is easy to *not* believe that at *least* a portion of the security which we seem to achieve is illusory.

CONCLUDING THOUGHTS

Probably, we must answer a fundamental question: How much should be revealed to produce an informed public and how much should be withheld in the Nation's intersest? In this context, there are many elements of society outside of government in which special arrangements exist to restrict the availability of information and to protect personal privacy – as noted earlier. Former Attorney General and legal academician Edward Levi referred to them in his presentation before the Bar Association of the City of New York in April of 1975. He dwelt on many aspects of the concept of privacy in an historical evolutionary commentary. He included, of course, such relationships as:

- Attorney-client
- Doctor-patient
- Journalist-source

- Income tax returns *vs.* "snoopy" neighbors.

These are examples of established relationships of confidentiality based on an individual's right to privacy and there is little question that these procedures should be preserved.

We all know that when the availability of information is restricted, opportunities for misconduct – public or private – is inherent. Wrongdoing can be concealed behind even the most justifiable of secrecy programs. I submit that intelligent, professional management of special access programs for reasonable purposes that are truly justified in the national interest will, axiomatically, serve the best interests of an informed citizenry. Why then the "bad press" effect we have come to know? When things go wrong, there emerges a common denominator which runs through the infinitely variable human – the tendency to blame someone else. Well, some modern minds reject the concept of original sin but, in a situation of abuse in this profession we must recognize ourselves when *Pogo* says:

"We have found the enemy and he is us."

SPECIAL ACCESS PROGRAMS – ARE THEY NECESSARY?

James J. Bagley
R. B. Associates, Inc.

Special Access programs have been with us for a long time – they grow and grow and grow. It is time to look at the structure of these programs to ascertain whether they are needed, are useful and whether they are effective in that they protect the information they were designed to protect.

A convenient starting point for examination is 1967, when the Freedom of Information Act was passed.[1] There is some opinion that the current rationale for such programs was a defense against the FOIA, but such opinion, frequently voiced in private, cannot be substantiated.

Special Access programs were officially blessed but not defined in EO 11652.[2] A cautionary note on the establishment of such programs was raised in the NSC Directive, of 17 May 1972, implementing the Order, which directed that all such programs "requires the specific prior approval of the head of a Department or his designee."

What *are* Special Access Programs? The term is defined in neither EO 11652, as noted, nor its successor new Order EO 12065.[3] Department of Defense Directive (DoD 5200.1R) provides the following definition: "A Special Access Program is any program imposing 'need-to-know', or special lists of persons determined to have a 'need-to-know'." The term "carve-out" is used widely in industry for such programs. The term is applied to any program where security responsibility has been retained by the User Agency.

The DoD policy as outlined in DoD 5200.1R on Special Access Programs states in part: "It is further the policy to apply the "need-to-know" principle in the regular system so that there will be no need for Special Access Programs requiring extraordinary procedures, and controls, such as formal access determinations, special briefings, reporting procedures and recorded formal access lists."

It is time for a critical look at the "cause and effect" of these programs. To begin, it is useful to raise questions which might begin to shed some light so that there might be an assessment on the effectiveness and utility of such programs.

- Do such programs need to exist?
- Does the government have (acquire, possess, control) information of such a nature that special extraordinary measures are needed to protect the information?
- Has the traditional "need-to-know" principle lost its validity?
- Are normal investigative procedures used to establish the trustworthiness of individuals adequate?
- Does the proposed program provide better security?
- Are the special procedures developed for these programs cost-effective?
- Are these programs controlled and surveilled by higher authority? Is there coordination and consistency in application of security procedures within the department and between agencies involved in the programs?
- What is the effect of these programs on the regular security programs of the agencies and their contractors?

As the term "Special Access Program" is ambiguous, an explanation of the term is useful. Section 4-2 of EO 12065[3] is quoted in part:

> "Agency heads listed in Section 1-201 may create special access programs to control access, distribution and protection of particularly sensitive information classified pursuant to this Order and prior Orders. Such programs may be created or continued by written direction and only by those agency heads and, for matters pertaining to intelligence sources and methods by the Director of Central Intelligence. Classified information in such programs shall be declassified according to the provisions of Section 3."

The remainder of the section prescribes the criteria for creation, review and continuation. It is pointed out, however, that the only requirement for coordination is for programs involving intelligence sources and methods under the direction of the DCI. There is no requirement for the coordination of programs approved by agency heads. Nor is there a definition of what kinds of programs may fall within the category of Special Access. It should be noted further that foreign programs, by definition, are special access inasmuch as there are special rules for access, control and dissemination.

It is fair to state that there will always be a need for systems to protect information of extraordinary sensitivity; whether relating to the affiars of state

obtained by a variety of means, or to the protection of individuals who could be in jeopardy if their identity became known. At the same time, remember, when a decision is made that a particular bit of information warrants special procedures for its protection, a companion decision must be made on the degree of protection required. This latter decision should involve:

- Segregating information based on its sensitivity
- Determining who must have the information and why. Determining whether the information requires separate clearance procedures for individuals involved in the program
- Determining whether special facilities will be required for the physical protection
- Assessing whether the existing security system of the agency is adequate
- Deciding whether the sensitivity of the information is worth the cost of protection.

Unfortunately, there is little evidence that these companion decisions are regularly made. It is far easier to declare (pontificate) that *all* the information is sensitive. That there is no difference between the measures applied to the protection of an individual, from the measures taken to protect information on a large program.

NEED-TO-KNOW AND INVESTIGATIVE STANDARDS

The common decision on a special access program is that all the information is sensitive. An easy way out. But is it a "good" out. As Ben Franklin once said, as noted by Maynard C. Anderson elsewhere in this Journal; "Three people can keep a secret if two of them are dead." If the sensitive information is such that it can be kept within a small circle of people the only problems are the trustworthiness and integrity of those people. However, if the program is one that involves several parts of an agency; the expenditure of public funds which are accountable; the involvement of contractors; participation of more than one agency or department; the possible involvement of other governments or international agencies; "need-to-know" then takes on far different dimensions.

In this day of micro-management, many different kinds of people have a legitimate need for information on any and all programs. Money managers need information on accountability of finances; auditors also have a need to comply with the multitude of laws and regulations on proper expenditures. When contractors are involved, they too need detailed information, particularly when there is a need for sub-contractors and suppliers who will need precise specifications on what is desired in order to construct a cost proposal. Should communications be involved, there must be an approval of the use of communications frequencies. Some require approval of the Federal Communications Commission, and, where international applications are involved, approval by the International Telecommunications Union.[4] These are only samples of the dimensions of "need-to-know" when applied to a large program. Each of these agents need to have information about a given program, regardless of sensitivity. And each need generally is based on specific requirements of law or regulation. In some instances is it a requirement that an agency publicize its intentions and wants.[5] Obviously, if a program is small, conducted with discretionary (little accountability) funds, "need-to-know" is simplified; it can be handled on a one-to-one basis and the only weakness is the possible lack of intregity of the participants. It also must be admitted that in these days of permissiveness, even integrity is becoming a forgotten word.

When one reads accounts of large programs, such as Project Jennifer,[6] being conducted as Special Access Programs one wonders how the managers ever expected to keep them under wraps for any length of time. In the case of Jennifer, one also wonders whether a project security guide existed, whether there might not have been a legitimate national and open requirement for a vessel as advanced as the Glomar Explorer – one has gathered that it was in the forefront of the state-of-the-art in ship design and on-board capability. Would not such a vessel be a national asset?

Turning to investigative procedures, the existing government standard for the determination of suitability for government employment is Executive Order 10450.[7] This Order was promulgated shortly after President Eisenhower took office as part of a new look at integrity in government; getting the "Reds" and "10 percenters" out of the government. Although there have been various attempts to update the Order, it is still in effect. With the rise of Special Access Programs there have been interpretations of the Order which led to requirements for more intensive and extensive investigations of individuals who would have access to such information. It would also be imagined that the frequency of leaks, compromises, espionage cases and whistle-blowers and the like have contributed.[8] Now there are Background Investigations (BI) and Special Background Investigations (SBI), the latter being required for access to Sensitive Compartmented Information (SCI).[9] It should be noted that it is possible to be eligible for access to Top Secret information on the basis of a BI and not be eligible for access to SCI which requires an SBI. An SBI is far more comprehensive in its scope. An examination of Appendix J to the Department of the Navy Information Security Program Regulation will reveal the

This writer does not know the difference in cost between a BI and an SBI, however, from the scope of the investigation, it would appear that the range would be from tens to hundreds of dollars. Not insignificant.

The problems of the investigations and their scope is highlighted by E.O. 12036[11] which grants to each of the members of the intelligence the authority have it own program which includes: "protection of the security of its installations, activities, information and personnel by appropriate means including such investigations of applicants, employees, contractors and other persons with similar associations . . . as are necessary." Even though the DCI is responsible for "the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information and products,"[12] there is still the possibility of a minimum of 12 separate personnel security investigative and clearance systems with each of the agencies involved having individual authority to act solely at its own discretion, with its own system and with its own resources. As written elsewhere[13] the structure of the Order permits – but does not encourage – the establishment of separate systems for marking, handling, protective systems and the like. One can imagine, without difficulty, that a contractor especially (it could also include the government) serving several members of the Community could be faced with differing and possibly conflicting requirements. It is easy to imagine also a scenario in which a contractor who builds a gadget applicable to several members of the Community having as many security requirements as there are customers and not being able to tell one that he was working for the other or that the gadget was the same.

BETTER SECURITY?

Security for Special Access Programs is handled generally by what is known as the Special Security Officer (SSO) system which is superimposed on the normal security system. It is the SSO organization which sets the standards for security that include investigative standards for access to the information within the system; it establishes physical security standards; and it disseminates information through a system of special controls. It is emphasized however, that even though the system was "blessed" by EO 11652[2] and carried forward by EO 12065,[3] there are still only three categories of classification – Top Secret, Secret and Confidential. Special Access information is only a component of National Security Information as established in those Orders. Although EO 12065 does not refer to EO 12036, it states clearly that: "This Order provides the only basis for classifying information. Information may be assigned one of the three designations listed below." This does not preclude the addition of caveats such as code or project names, restrictions on further disseminations, *etc.*

The question is whether these additional requirements and measures provide any better security than the system to provide for other national security information. The requirements of the system are set forth in EO 12065 and its implementing Directive (to be published),[14] and the various implementing directives of the departments and agencies which will be public documents. It is these directives that govern protection, establish standards for all who have access to national security information. As well may be imagined, with each of the members of the Intelligence Community issuing its own creations, chaos can be the result. And well it may. It could be a reversion to the days prior to the issuance of the Industrial Security Manual for Safeguarding Classified Information.[15] At that time each of the procuring activities did issue their own rules, conducted their own inspections and had their own singular requirements, and did not recognize the existance of any other agent. Obviously, industry could not operate under such conditions and pressed for a single standard. By agreement, the provisions of the ISM are applicable to most of the agencies and departments of the government. The most notable exception of course is the Department of Energy which is governed by the Atomic Energy Act of 1954,[16] as amended. Even there, there is general consistency between the DoE and the DoD standards including the issuance of a number of joint DoE-DoD Classification Guides.

Although the recent years have brought considerable consolidation, the recent trends away from consolidation and toward oneness – each agency doing its own thing – individual access requirements, clearances, physical security standards, *etc.* An individual cleared for access to a program of one department could be denied access to the same program information in the possession of a cooperating agency. The review and evaluation process easily could be different from one agency to another to the end that an individual cleared for access by one agency could be denied access by another and all based on the same investigative information. How could a contractor producing a single product for agencies be affected by differing agency standards? It is possible for one agency to require a vault that will be of four-inch thick reinforced concrete and another to require it to be six inches thick; that reinforcing rods be one quarter inch in diameter *vs* one half inch. That there would be a substantial cost difference is obvious, not to mention the difficulties in serving several masters. The point of all this is that there *is* no requirement that individual security systems established by each of the members of intelligence community be reviewed for consistency. There is only the requirement that the DCI coordinate the programs under his authority.

The basic question remains – do the security requirments established for Special Access Programs provide better security? Here, it is fair to say that the

evidence is *NO.* Some of the biggest security leaks or busts have come from these programs. It can be concluded that in a program in which *all* information is sensitive that no infomration is sensitive. When a participant who does not know what is sensitive and tries to protect everything, is pressed for information he or she cannot discriminate between that which is from that which is not. As to the cost – there is no evidence that increased personnel and physical security requirements have accomplished much. People are still people; trust is still trust and integrity is still integrity. None of these are susceptible to quantification or precise qualification; morality has never been successfully legislated.

COST EFFECTIVENESS

It is frequently said that security is a non-productive overhead cost. This probably is true – except when there is a "bust" and the powers heap their wrath on their security managers – How, Why, You failed, etc. But the fact remains that security is an overhead cost that is frequently cut in times of relative peace. Then too, security frequently is the lowest paid, has the most difficult time in defending grades and frequently is the victim of the cost cutters. It is not the point here that security managers have taken their revenge by establishing empires in the administration of Special Access Programs. But, to my stated question, what *is* the cost of security in these programs? There is little knowledge of how many programs there are throughout the government and less knowledge of the details of the programs and the management, therefore, it is difficult to establish a base point from which cost might be computed. One must say that evidence is not available to reach a conclusion.

It is pointed out again that EO 11652[2] authorized the programs to be established without a requirement for coordination. The structure in the NSC implementing directive[3] that such programs could only be established by the authority of the head of the agency or his designee added little in the way of control. The new Order – EO 12065 does establish a new control process for Special Access Programs. For example, criteria for establishment are set forth along with a review process and automatic termination dates, and a review procedure for programs in existance at the effective date of the Order (1 December 1978). However, the control mechanism is contradicted by the provisions of EO 12036 which authorized the members of the Community to go their own way and do their own thing. As there are no words in EO 12065 to assure its primacy over companion Orders (12450 and 12036), it would be assumed that the Community would go its own way under the authority already in existing Orders. How then would it be possible to ascertain cost of any program which by its nature is kept under wraps with even the overall cost of the program frequently classified.

WHERE TO GO

As the Red Queen said in Lewis Carroll's *Wonderland,* "Now *here* you see, it takes all the running you can do to keep in place. If you want to get somewhere else you must run at least twice as fast as *there.*" Although there are no valid statistics on the number of Special Access programs in effect throughout the government, there is agreement that the number has increased markedly since 1965. A "reliable source" reports that there are several hundred such programs. If there is such a number, and each with its own security organization, one can imagine that the cost would be very high.

It is readily apparent (and generally without argument) that there will always be a need for such programs – the protection of important sources and equally important assets is paramount. With the need apparent the next step is control and management. A major question is whether there is a need for separate organizations to protect the information. Would it not be appropriate to look at the programs and assess the cost and effectiveness of the protection versus the importance (value) of the program to thy national security? Here one must fully recognize that it is very difficult to assign a cost value to protection, particularly when the *information* being protected is not susceptible to a price tag. It is recognized also that there will always be variables in the kinds of protection given to different kinds of information. For example, if there is a source "in place" providing information of great importance whose life depends on the protection of his identity. Clearly protection would be considered an absolute limitation on the individuals who have knowledge of the identity, or information from which one could glean or surmise the probable location of the source. Clearly also, extraordinary measures might be required to protect such a source. Contrast that situation with a research and development project costing in the multi-millions; requiring a large number of subcontractors and suppliers; interagency support; products which cannot be hidden from view; large scale test and evaluation; and final results which are of importance to many activities.[1 7]

Elsewhere in this Journal is an article, "The Case for Special Access Programs," by Maynard C. Anderson which makes the point that he suspects that Special Access Programs were developed because the principle of need-to-know was no longer effective. This writer cannot accept abandoning the principle. In fact, it is my belief that if the principle were to be correctly applied now, there would be no need for special access programs – essentially a point made also by Mr. Anderson. Undoubtedly it is more difficult to apply these days than it was. The need for information is so extensive – budget analysts need program information to prepare requests for appropriations; engineers must justify their requests for funds for the construction

and maintenance of facilities that must be used for a program including one that must be protected; position classifiers must have information in order to apply a proper grade or salary level to the respective jobs. Each has a legitimate need for some program information. How this need may be satisfied and still protect sensitive information is a difficult and complicated question – but the answer in each case must be found. In the past it was convenient to wrap the program in its own cocoon or put it behind a "green door," or in a "black box," give it a code name (classified naturally) and hope the hard questions would not be raised No more. These days the information security officer must know from the beginning what the program is; what information must and should be protected, and for how long; who needs the information and why; and, of the greatest importance – what is the bottom line? What information must be protected at all costs. This is "need-to-know." It is also the balancing test now required. Openness is a fact of life and applicable to all parts of government, including the intelligence community.[18] In the future the determination of need-to-know will require greater precision and frequent examination; however, the principle is still valid and must be given new life.

POSSIBLE AVENUES OF EXAMINATION

There are now two types of background investigations: For access to Top Secret information a regular BI *is required.* For access to Sensitive Compartmented Information (SCI), a Special Background Investigation is required.[9,10]

1. Why should there not be a single standard for a Background Investigation? If the present BI is not adequate to determine trustworthiness to handle national security information and an SBI is, why not use the same standard. After all, there is no higher category of information sensitivity. Parenthetically, there has been a continuing pressure to reduce the number of individuals having access to TS; a more comprehensive and certainly more expensive investigation could be one way in helping to reduce the number of holders.

The requester of an investigation could be required to reimburse the investigative agency for the cost of the investigation. Having to pay for an investigation would tend to reduce the number of requests.

2. Classification guidance must be a requirement. With some exceptions (based on an appeal to the Information Security Oversight Office (ISOO)) EO 12065 does make guidance a requirement. There should be no exception for Special Access programs or Cryptologic programs under the control of the Secretary of Defense. To the extent appropriate, there should be interlocking classified and unclassified guides, widely distributed, so that all participants both government and industry, would know what is sensitive and for how long.

Guidance must be kept current. Should the failure to keep guidance current result in embarassment, leaks, unauthorized disclosure and the like, such failure could be the basis for disciplinary action for all concerned regardless of the level or sensitivity of the person responsible.[19]

3. Physical security standards should be reviewed for consistency. There should be a single basic standard for all participants, government and industry related to the sensitivity of the information or material requiring protection. If there should be a requirement for increased standards, they should be subject to review and require approval by an oversight agent such as the ISOO. If approved the cost of the increased requirement should be borne specifically by the requiring agency.

4. All established security standards should be applicable to both government and industry. There is no valid reason why the government should impose standards on industry that it does not require of itself. Examples of dual standards are numerous – Among Departments and Agencies and between them and even a given contractor serving several of them.

CONCLUDING OBSERVATIONS

In the last decade there has been a marked increase in the number of Special Access programs. They were started with the intent of providing a greater degree of security to program information. Were they successful? Were they worth the cost? Did they reduce the number of "leaks" and "busts?" It is fair to say that the answer is NO. There still are leaks, espionage cases, and sales of classified information by people who were cleared for access after an expensive background investigation. Of greater importance to the overall national defense is the charge that "security safeguards impede federal prosecutors."[20] In the final analysis, it appears that the special investigative, access and protection requirements are no better than the standards applied to other national security information. Perhaps there should be a better recognition that there is not yet a lock that can secure the minds of men. What is the answer? Obviously the security system has lost credibility at a very critical time in our history when old values are being questioned and in some cases discarded – for better or for worse. To dismantle the system would be catastrophic. However, there are steps which might be considered and taken by reasonable people. The following are some of the steps which might be considered:

- Establish a legislative basis for the classification system. NCMS has long recommended such a course.

- Establish penalties for the unauthorized disclosure of classified information which are applicable to all branches of government and all who have access to national defense information

- Require that agencies imposing additional requirements will pay specifically for the cost of additional requirements.

To date there appears to be no valid justification for the imposition of the additional security system authorized for each of the members of the Intelligence Community and the Head of any department or agency authorized to establish a Special Access program. At the risk of invoking another tired old cliche – *it's time to take another look at the system and make changes.* Possibly a look by representatives of the three branches of government augmented by interested outsiders who have special knowledge of the problems could be a starting point. It is always nice to approach the problem from an ivory tower, but a look at security as it is actually practiced would be an eye-opener. As stated by Elliot Richardson in his book, *The Creative Balance.*[21]

> *"Here again, as in every other area of important public concern, we have no realistic choice but to allow room for good common sense and wise judgment of those to whom we have delegated responsibility. Nor does the fact that this truism has sometimes been abused make total distrust a workable alternative."*

REFERENCES AND FOOTNOTES

1. The Freedom of Information Act, 4 July 1967 (5 USC 552) as amended by the 1974 Amendments (P.L. 93-502)
2. Section 9 Executive Order 11652
3. Executive Order 12065, signed 28 June 1978, effective December 1, 1978
4. The International Telecommunications Union, the United Nations specialized agency which provides standardized communications procedures and practices, including frequency allocations assignments and radio regulations on a world-wide basis.
5. Armed Services Procurement Regulations, 1976 edition. Paragraph 1-1003.1b states: "Only those classified procurements, where the information necessary to be included in the Synopsis [Commerce Business Daily] cannot be worded in such a manner as to preclude the disclosure of classified information, or when the mere disclosure of the Government's interest in the area of the proposed procurement would violate security requirements, shall not be publicized in the Synopsis. All other classified procurements shall be publicized in the Synopsis, even though access to classified matter might be necessary in order to submit a proposal or to perform the contract. The intent of the exception for classified procurement in the synopsis requirements of P.L. 87-305 is not to exempt every classified procurement from publicizing, but to provide a safeguard from violating security requirements."
6. "Project Jennifer," *Parade Magazine,* Lloyd Shearer, May 11, 1975, also various articles in the *Washington Post, Newsweek, New York Times, et. al.,* March through May 1975.
7. Executive Order 10450, "Security Requirements for Government Employment," 27 April 1953 (18 F.R. 2489)
8. The defection of NSA employees William H. Martin and Bernon F. Mitchell in August 1966; the suicide of Sergeant First Class Jack E. Dunlop when he learned he had been discovered selling NSA documents to the Soviets; convictions for espionage by persons who had been cleared for access to intelligence programs, *etc.*
9. Sensitive Compartmented Information (SCI). Recently this term has come into general useage. The Industrial Security Manual (ISM) CH.1 5220.22-M defines SCI: "This term includes all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. This term does not include RESTRICTED DATA as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended."
   NOTO BENE: The word "community" is used 3 times in the definition but is not, of itself defined in the ISM. The term is defined in section 4-2 of EO 12036 and shall not be repeated here.
10. OPNAVINST 5510.1E, Department of the Navy Information Security Program Regulation.
11. Executive Order 12036 of January 24, 1978
12. Section 1, Paragraph 106, EO 12036, Director of Central Intelligence
13. NCMS *Bulletin,* Vol XXII, Number 2, Mar-Apr 1978
14. At this writing, the NSC or ISOO Directive implementing EO 12065 has not been approved. The standards in reference 2 are applicable.
15. The Industrial Security Manual (ISM) establishes security requirements for industry. By agreement with the DoD, the ISM applies to contractors of most of the executive agencies and departments. A listing may be found in the Manual.
16. Atomic Energy Act of 1954, as amended.
17. The Glomar Explorer. A prime example of a vehicle which certainly involved a substantial amount of advanced research and development, a type of oceanographic vessel which had not previsouly been built and which represented an advance in the state-of-the-art in search and rescue, and exploration and recovery vehicles. There had to be cooperation between agencies involved in the oceans as well as cooperation with the shipbuilding industry. Substantial argument could be advanced that the primary purpose of the vessel was of

lesser importance than the development of a vehicle of such sophistication. Regardless of the cost and regardless of the primary purpose, such a vehicle might well be considered as a unique national asset.

18. President Carter, in a talk at the Central Intelligence Agency on August 16, 1978, made the point that the intelligence community did have the responsibility to conduct its business in an atmosphere which required not only security, but openness; that the balancing principle which was established in EO 12065 had to be applied to intelligence matters.
19. *U-2 Affair,* David Wise and Thomas B. Ross, Bantam Books, November 1962. There was a breakdown in the cover story between participating agencies. As the book points out," When disaster struck, the government was not ready, even though the program had been running for many years. As a result it stumbled into a series of errors."
20. *Washington Post,* August 20, 1978. A story on charges affecting employees of Lockheed, ITT and CIA, that were dropped because a trial would have compelled disclosure of classified information.
21. Elliot Richardson, *The Creative Balance,* Holt, Rinehart and Winston, 1976

STRUCTURE AND PROCESS IN FORMING NATIONAL SECURITY POLICY[1]

An examination of the process by which national security policy is formulated and the influences of the pluralistic society on that process. An appraisal of the national defense structure, the role of non-military sectors of the society in formulating policy through the dialogue of competition for limited resources and the part played by the media, labor and the Congress in the formal and informal structures. An assessment of the provisions, within the system, for corporate memory and institutional foresight.

Chairman's Plenary Session Summary

Honorable Brent Scowcroft,
LTG, USAF (Ret.)

The panel on structure and process was peopled uniformly with strong panel members having strong views on every aspect of the subject. The discussion was invariably lively, albeit sometimes distinguished more by heat than light. I will try to be careful, at pain of public disavowal, to represent the panel's views on the various things that we discussed.

It was very difficult for us to get a handle on something so, on the one hand, cohesive and on the other amorphous as structure and process. In many respects we thought we were like the six blind men defining the character of the elephant. But armed with two outstanding papers, we felt our way into the topic.

At the outset it was suggested that maybe we should decide what it was that we were talking about. That was followed by a lively discussion on the meaning of the term "national security," especially in view of the fact that in the past the term had been abused perhaps.

One of the papers presented to the panel pointed out the growing interdependence and mingling of things traditionally felt to be foreign and domestic and that the framers of the National Security Act of 1947 had, in fact, a very broad view of what was encompassed within the term "national security." It was suggested that "national security" could be defined as "a process of protecting all the assets, national interests, and sources of power necessary to secure the nation's well-being from threats — military, economic, and political — using appropriate resources."

Even with a definition such as this, we felt it was difficult to place any given subject either inside or outside the term "national security." It was suggested also that national security be viewed as one part of a continuum, following the goals specifically designed with survival of the nation at the one hand, blending down into issues dealing entirely with quality of life at the other. But there was no clear place on this continuum that you could delimit or mark a boundary of national security. It was noted that it had expanded to include issues such as global poverty, which had been felt earlier not to be a matter of particular national security concern for the United States.

Other issues, such as energy and nuclear proliferation, have, of course, both very intense domestic and national security implications, so we did not arrive at anything all that specific but did observe that national security had a much broader context now than had been felt previously.

We did discuss quite explicitly whether a definition should include reference to domestic aspects of national security. I think the panel felt definitely that there were domestic aspects to national security, and there was some attempt to include them in the definitions that I have set forth. But, in view of the sensitivity of that aspect, and the feeling that a description would have to be so carefully honed and delimited, we did not make that attempt.

As a way to get inside structure and process, which, if you pull it apart in a way you destroy what it is you are looking at because each part interacts with all the other parts, we decided to look at the principal actors in the process — the President, the Executive Branch, the Congress, pressure groups, and public opinion.

Starting with the President, there was a clear consensus that the President is the preeminent actor, certainly within the Executive Branch, in national security policy formulation and, therefore, that the particular structure of national security policy machinery would depend mainly on the President. It had to be something that he could or would use and feel comfortable with because the process was highly personality-dependent.

We felt that any structure should provide the President with:

- accurate information which he wants, needs quickly;
- all reasonable options on the issue under review;
- views of all principal advisers and agencies; and,
- some kind of mechanism to oversee the implementation of Presidential decisions.

[1]This paper was, in fact, Panel 5 of the *National Security Affairs Conference — 1977*, held at the National Defense University, July 18–20, 1977. It was contained in their published *Proceedings* and is included here with their agreement. Its content is believed to be pertinent to the members of the Society in the performance of their increasingly difficult tasks.

How this should be done was not discussed in the sense of a disposition to tinker with wiring diagrams or with the details of a structure, especially within the Executive Branch, for national security decisionmaking. I think this is a reflection of two things — first, that the machinery over the years has evolved into something that there is no great disagreement with; and second, in recognition of this preeminent role of the President, that he must be the one to develop the machinery or to use the machinery that is extant in the way in which he will be comfortable.

There was some discussion on (avoiding constitutional issues) compelling the President to receive advice from one or more people in different parts of the process. The feeling of the panel was that while there was no way that the President can be compelled, in making a decision, to accept advice from any or all of his advisers, the mere fact that he had to sit down and face or listen to one or more advisers — be it the Chairman of the Joint Chiefs, the Secretary of State, whomever — would provide an additional brake on hasty decisionmaking, and further, ensure that all points of view would be heard.

The panel also looked at the relationship between the President and his personal advisers — whomever he selected, whether they had a formal or informal position within the government — and the bureaucracy itself. We felt that there were, by the very nature of the bureaucracy, pressures which naturally tended to impel the President to rely more heavily on a personal staff or on personal advisers as opposed to the bureaucratic machinery itself.

The panel felt that there was no guarantee that the agencies would or would not be brought into any particular issue in a bureaucratic way, that part of it depended on the nature of the issue itself, on the time available to make the decision and, in a sense, on the secrecy which the President or other actors felt was required in making the decision.

It was also felt that a decision with which the bureaucracy or elements of it were not in sympathy could cause grumbling, disaffection, leaks designed to negate the policy, and that this frequently would be an element in a decision not to use it. The panel felt, however, that the bureaucratic machinery was a vital resource. It always provided the function of keeping its own agency head abreast and aware of issues so that if the President decided on a more informal kind of decisionmaking process, the agency heads, the personal advisers that the President may call on, would themselves be able to provide these necessary attributes for a useful decisionmaking process.

The panel was greatly concerned as well with the problem of introducing longer-range thinking into the decisionmaking process. And it was felt that perhaps this was a role that the bureaucracy could play which had not been fully exploited. There was full recognition of the difficulty of getting a grip on longer-range planning, the understanding that long-range planning staffs frequently become sort of ivory towers, totally outside the process, and therefore ignored; or, if they are successful, they tend to be coopted into the immediate decisionmaking process and lose the time and capacity to make longer-range projections.

While we didn't come to any real conclusion, I think we felt that perhaps a rewarding way to do it — rather than to set up separate staffs for long-range planning — was to make cognitive changes on the part of the staff. These would have to come from the top — from the agency heads, or from the President himself — to structure a bureaucratic reward system, and to provide a premium for presenting longer-range implications of decisions and policies. We all recognized that such an approach was likely to take a matter of some years — even if pursued assiduously.

We dealt at considerable length with Executive-Congressional relations. In general in this process, we skirted the questions of constitutionality. We discussed the War Powers Act, for example, at some length but without attempting to get into any kind of a determination of whether any particular role was or was not constitutional. We had very interesting discussions, bolstered by an outstanding paper on this issue, but we did not try to resolve the question. We did generally agree, however, that the Congress' constitutional role should be strongly supported and that while for constitutional and organizational reasons we did not feel they could be involved in the details of substantive policymaking, greater efforts should be made to provide them with information. I think this was based on the sense that they sometimes acted from insufficient information and to aid in resolving what the panel felt was a significant problem pervading the whole arena of national security policymaking at the present time — namely a sense of distrust between the Executive and the Legislature — a sense of suspicion and distrust. They believe that, in a broader sense, the public itself distrusted government and all larger institutions. That whatever the particular merits of the Executive-Legislative balance at any given point, it was important to make efforts to somehow break down this sense of distrust. A more open attitude toward providing Congress information would help. There was no great feeling, however, that this would in fact greatly diminish what I think at least most of the panel felt was a sort of struggle for power at the present time between the Executive and the Legislature stemming from past events but broader than any particular thing.

We were handicapped by not having a member of the media present on the panel, so they didn't fare quite as well as some of the other actors. We felt generally that "the media" was difficult to define; you

could put it, depending on your predilections, either as a pressure group or within public opinion. We recognized that whether you felt it was a creator or a transmitter of opinion was of substantial importance in this whole process. That fact was apparent to all of us. What we did not agree on is how the national security structure could or should deal with it. That question remained essentially unanswered.

In connection with this attitude of mistrust within the country, it was generally felt that the government as a whole had to live and operate more "in the sunlight," as one panelist expressed it. This stimulated considerable debate. For example, does not the public already have more information available to it, impressive fractions of which it ignores? Can it absorb more? What is the feedback? What do you expect from more information? How does the government protect what the panel felt was absolutely essential — and that is the Presidential advisory process in opening itself up? And would not the government opening up, leave itself open to charges of propagandizing the people in favor of its own ideas?

Nevertheless, I think most of the panel felt that there should be a more open policy for dissemination of information. A number of the panelists felt that the Executive Branch should make a fuller explanation of the choices that it faces, their anticipated costs and consequences, even if by doing so occasionally the ensuing debate would close off a favored option. In other words, that the Executive may have to sacrifice a certain amount of effectiveness for the sake of legitimacy. As I say, this was perhaps the most controversial of our discussions, and we all realized the difficulties and the pitfalls in this recommendation and the essential antagonism between some of the actors in this process.

Just by way of summary, I think of the five actors, certainly we felt the President was by far the strongest in terms of the determinations of the policy itself; that the Executive agencies themselves played a considerable role in underpinning the policy — in developing it and in providing an expert basis for it.

We felt also that pressure groups could be extremely effective but usually only on a narrow front on particular issues. The Congress and public opinion — I think generally it was felt that in the day-to-day operation of national security decisionmaking, they were not as strong certainly as the Executive Branch. Generally, they were not as strong on individual issues as pressure groups could be. We recognized that pressure groups, for example, would work through the Executive Branch, the Congress and public opinion in achieving their particular aims. However, the Congress and public opinion possessed gross tools which on particular issues could substantially change both the direction and the character of national security decisions.

Rapporteur's Report

LTC Thomas A. Pianka, USA

The panel agreed that it would be useful to begin its discussion by attempting to define at least in general terms the meaning of the term "national security." This seemed especially necessary because of the widely-held perception that in the recent past the term had been abused. One of the papers prepared for the panel underscored the growing interdependence and mingling, in recent years, of "domestic" and "foreign policy" issues. It was also pointed out that one need only glance at the 1947 National Security Act to realize that its framers had a broad view of the meaning of national security. In the spirit of the broad view, one panelist suggested the following definition: National security is the process of utilizing the appropriate resources to protect all the assets of power necessary to secure the nation's well-being from foreign military, economic, and political threats.

Even were this definition to be accepted, the panel felt that it remains difficult to place any given issue inside or outside the domain of national security. One panelist suggested that the concept of protection is the essence of national security: The national security process entails looking at goals or interests with a view toward their protection. It was further suggested that national security be viewed as falling on a continuum of national goals, with national survival as one extreme which is clearly identifiable as a "national security" issue, moving toward issues dealing chiefly with the quality of life, at the other extreme. Especially in the present age, which as previously noted, is characterized by an increased comingling of issues, it is difficult to cut this continuum at any one point which would clearly delimit national security and separate it from other national goals. National security may expand to encompass issues previously considered to be outside its purview. Global poverty, it was suggested, is an issue which is now seen to have previously unperceived national security implications. Other issues, such as energy, may move along the continuum toward the national survival extreme and assume additional national security aspects which they once lacked. Finally, new issues may arise, such as nuclear proliferation, with clear implications for national security. Through these various processes, the panel agreed, the mantle of national security has indeed come at the present time to cover potentially a considerably broader range of issues than it had at any time in the past.

In its discussion of definitions, the panel recognized that threats to national security may arise in the form of unconstitutional or extraconstitutional domestic challenges — *e.g.*, terrorism, subversion, the advocacy of violent overthrow of existing institutions and the

like. However, in light of the complexity and sensitivity of these issues, it was felt that it would be more profitable to concentrate the panel's attention on the national security process in relation to the more clearly perceivable and definable parameter of foreign threats.

Having reached an acceptable working definition, the panel decided that it would be useful for its deliberations to discuss structure and processes in national security policymaking in terms of the five major actors involved: the President, the Executive agencies, Congress, pressure groups, and public opinion.

There was clear consensus that the President — defined as the "institutional Presidency," including the Chief Executive and his immediate staff — is the preeminent actor in national security policy formulation. This preeminence results from the nature of foreign affairs in general and, as one of the papers prepared for the conference emphasized, the historical development of American constitutional theory and practice.

The panel also agreed that the structure within the Executive Branch for national security policy formulation depends mainly upon the President and his personality: it must be something he can use and with which he must feel comfortable. Whether the structure is formally designed or evolves, it is dependent upon the President's personality. Any established organization for policymaking, even if it happens to be legislated,* may be supplemented or bypassed by a system the President finds more suitable. Moreover, the formal system, whether it is legislated or otherwise developed, may or may not be the primary vehicle for national security policy decisionmaking. Many issues (or perhaps only selected ones) may actually be decided outside the formal system. Some panelists recalled Dr. Kissinger's 1966 article in which he pointed out the necessity of sometimes keeping the development of major policy departures secret from the established system; a technique most dramatically employed in President's Nixon's opening to China.

Given the decisive influence of the Presidential personality on the policy process, the panel agreed that a staff's duty is to adapt to the President's needs. As one panelist expressed it; "it is fruitless to try to 'reform' the President." If he is disorderly, the staff must work all the more assiduously to ensure order in the system. Another panelist felt that all established systems eventually break down and that *ad hoc* systems will evolve. It is the task of staff personnel, he felt, to adapt to this: it must "staff the Tuesday Luncheon," so to speak, if such an affair becomes the primary means of conveying advice to the President on national security problems.

*Emphasis supplied — not in the original.

In any case, it was agreed that any structure should:

- Provide the President with the information he requires quickly and accurately;
- Present all reasonable options; and
- Present the point of view of all principal advisors to the President.

The precise structure should function in such a way that the President will be encouraged to use it because it allows him to make the most informed decisions possible.

The panel also agreed that the structure should provide a means for monitoring the implementation of decisions. There was no clear consensus, however, as to whether this could be more effectively accomplished by an entity on the President's staff — similar perhaps to the Policy Coordinating Board of the Eisenhower Administration — or by the operating Cabinet and agency heads. Some panelists suggested that a system for critiquing the implementation phase of the policy process would be useful.

The panel devoted some time to discussing problems that may arise in relations between the President's personal staff and the larger bureaucracy. It was felt that inherent slowness in responding to requirements and the possibility of dissent — whether for legitimate or shortsighted reasons — on the part of the bureaucracy impel a President to depend more heavily on his personal staff or advisors than on the bureaucratic machinery. This is inescapable, given the President's preeminence in foreign policy, the human inclination to acquire an inner circle of trusted advisors, and the attitudinal and administrative tendencies which are familiar from the "bureaucratic politics" literature, that encumber and slow down the response capabilities of the departments and agencies. These inherent and timeless weaknesses of the larger bureaucracy are reinforced by advances in new technologies of communication, transportation, and data transmission which in many instances compel quick decisions and immediate action. The panel also discussed the inner workings of the President's staff and advisory circle and concluded that absolutely smooth and friendly relationships among the principal national security advisers is not a prerequisite for effective policymaking. In fact, and again depending upon the personality of the President, a certain amount of "creative tension" among them may not be unwelcome in that it may tend to illuminate more fully the options available and their costs and consequences.

There was considerable discussion of the necessity to bring political considerations early and effectively into the policymaking process. The panel addressed more fully the need for openness in the system later in its discussions, but at this point, it generally agreed that the political ramifications of a policy under consideration be an integral part of the decisionmaking process.

As alluded to previously, the larger bureaucracy of the Executive Branch departments and agencies may or may not be brought substantively into the policy formulation process. This will frequently depend not only upon the nature of the issue, but on the time available for decision, as well as the President's predilections. The consequences of this fact were discussed at some length. Exclusion of the bureaucracy from effective participation in the process may cause grumbling, leaks designed to counter policies upon which the agency was not consulted or with which it disagrees, and lags — often deliberate — in the implementation process. In other words, the bureaucracy is not without weapons in this struggle. On the other hand, the President is far from powerless in countering or foreclosing such actions on the bureaucracy's part. It is a simple matter, and a technique sometimes used in the past, to hold formal meetings to ratify or "legitimize" decisions already taken in private or within a closed inner circle — a form of "stroking" the bureaucracy as one panelist expressed it. Bureaucratic maneuverings of the past notwithstanding, however, the panel seemed generally to agree that the best system provides for full and real presentation of the views of all principal statutory advisors and the organizations they represent in order to ensure the best informed policymaking process. Whatever the particular involvement of the bureaucracy in a specific case, it still performs the vital function of keeping the various department and agency heads as fully informed as possible with the background information they require to fulfill their function of advising the President. At any rate, the panel felt that despite the inherent cumbersomeness of the machinery, the bureaucracy represents a vast fund of knowledge, information, and expertise, and the President and his staff should make strong efforts to use its potential effectively.*

The panel also addressed at some length the problem of building into the policy formulation system a capacity for anticipatory deliberations, *i.e.*, a capability for a longer-range look at potential or burgeoning issues. Put another way, can long-range policy planning be satisfactorily integrated into the decisionmaking process? Experience has repeatedly demonstrated that policy planning staffs, if relatively ineffective, degenerate into ivory towers whose personnel, deliberations, and products are ignored. If they are effective, on the other hand, they tend to be drawn into the maw of current events and crises. Some panelists also pointed out that it is difficult to establish the relevance of long-range planning and another stressed that all planning should affect today's operations or it ceases to be useful. For these reasons it was generally agreed that long- and short-range planning and policy formulation should not be organizationally separated and that separate entities for the longer perspective are best avoided. Rather than being a piece of institutional turf, long-range planning, in the expression of one panelist, should be a habit of mind. It is better to encourage cognitive changes on the part of existing staffers, to seek to impart changes in their mind sets which will impel a longer-range perspective. Moreover, success can be expected only on occasion and only on the margins. Even this is an admittedly difficult order and many panelists were not sanguine concerning it. Based on the experience of private business, it would seem that this desirable if difficult change depends upon revising educational processes, both in the general educational system and within the organization's training program, changes in the incentive systems within the organization to reward the longer-range perspective and the strong and sustained interest of the Chief Executive.

The question of how well the Executive Branch can be expected to develop a purposeful and coherent strategy, with due consideration and concern for the long range, and the role of the Congress in this process, was discussed at some length. Substantive questions such as containment and detente, Cyprus, Angola, and the Indian Ocean were brought into the discussion in order to illuminate the issues involved in this problem. Some participants pointed out that the implementing agencies, especially their planners and operators, need clear policy guidelines. However, other panelists noted that detailed long-range planning is either anodyne or implies or conduces an activist interventionist role unsuited to a power like the United States which does not seek world domination. In general it was conceded that the formulation of long-range strategy is difficult, especially in detail. Nevertheless, the panel generally agreed that a stronger effort should be made to seek long-range continuity and coherence in foreign policy, *i.e.*, to project ahead and to integrate as much as possible goals and operations, plans, and actions.

The panel discussed Executive-congressional relations at length. It became clear in this discussion that, because of congressional sensitivity to constituent and media opinion and to interest group pressures, the Executive's relationships with all three actors are closely intertwined. The panel did not question the necessity and desirability of providing for the constitutional role of Congress in the foreign policy formulation process. It was generally agreed, however, that it is infeasible, as well as of dubious constitutionality, for Congress to be involved in the details of substantive policymaking. Because of its inherent organizational character, Congress cannot be a mirror-image of the Executive

*Emphasis supplied.

Branch and it cannot aggregate interests into a coherent policy. However, subject to maintenance of secrecy for constitutionally protected advice given to the President, the Executive Branch must make a greater effort to supply more information to Congress, through declassification of information where possible and necessary, and through other devices. The panel did not believe that such an effort would quickly solve the present conflict between the two branches, but a more frank and open dialogue between the branches could over time rebuild a more cooperative and fruitful relationship.

However, for Congress to play its legitimate role effectively, the public must also be kept informed and, of course, the media cannot be ignored in this process. The resolution of national security issues often requires not simply "permissive consensus," but rather a positive stand on the part of individual Senators and Congressmen. (In this connection, some panelists pointed to a serious dilemma for Congress — does it and should it *lead* or *follow* public opinion?) At any rate, public opinion will be a major determinant of how Congress reacts to the Executive lead in national security policy issues. Moreover, a substantial portion of the old foreign policy consensus, anchored essentially in the containment policy, has broken down. One panelist pointed out that large numbers of people reject both containment and its more recent partner, detente, preferring instead a form of isolationism. The panel also recalled from its earlier discussions that foreign policy issues are not often intertwined with domestic issues having powerful constituencies, some broadly based and others depending on single issue pressure groups which may be more narrowly based but have the advantage of a tight and disciplined focus. Furthermore, Congress, reflecting the society at large, is now more pluralistic, and there has been a substantial decline in its inner discipline, making consultation and agreement between the two branches both more difficult and less assured. Thus, the Executive must make efforts to inform the public more completely — which is accomplished most often through the media — in order to strengthen the cooperation of Congress.

There was considerable debate and some disagreement as to the nature of the media; *i.e.*, is it merely a business or literally a Fourth Estate. Further discussion concerned the degree to which its opinions tend to be monolithic or characterized by a predictable sameness. The exact degree of its effect on public opinion was also subject to some disagreement. The panel did agree, however, that the media are extremely important whether as creators or transmitters of opinion. Television especially, because of its intimacy and pervasiveness, is of overwhelming influence. The fact is that the media are there: The question is how does the national security policy structure deal with them? That question remained unsolved in detail, but the panel agreed with one member that rather than "subverting, overriding, coopting, or faking out" the media and the public, the system must live with them honestly.

The panel felt, then, that the government must learn to live and operate more openly, "in the sunlight" as one panelist suggested. There was considerable debate on the details of operating "in the sunlight," however, and a number of doubts were raised.

- Does not the public already have available a great deal of information, most of which large fractions of the public ignore?
- Can it absorb more information?
- How is the feedback to be gauged?
- How does the government protect a President's advisory process — without which he will not be able to get the assistance essential to sound and informed decisionmaking?
- Finally — and most of the panel found this point deeply disquieting — would not the government open itself to charges of propagandizing its own people were it to provide more information with a view to seeking increased support for its policy decisions?

Nevertheless, most of the panel agreed that the current national mood of distrust and suspicion decrees that the national security policy process must be more open, that there should be less secrecy, and that a greater effort must be made to keep Congress and the public informed. As already noted, there was strong support for protecting Presidential advice and counsel. Most felt, however, that the Executive Branch must provide a fuller explanation, not of the deliberative process itself, but of the choices it faces in national security affairs and their anticipated costs and consequences. (This would have the additional welcome effect of forcing the system to think through the costs and consequences of proposed policies more thoroughly than had sometimes been the case in the past.) This is necessary even if by doing so the Executive will see a favored option foreclosed or suffer an occasional reversal of policies it prefers. In short, the Executive may have to sacrifice a certain amount of effectiveness for the sake of legitimacy. The panel recognized the difficulties and pitfalls in this recommendation. The issues are complex and not easy to explain. Adversary relationships between the branches and among the various and multiple nodes of interest and power within the body politic will ensure that information provided by the Executive will be used selectively to support preconceived positions. Nevertheless, the general desire on the part of the citizenry for a sense of participation and for knowing what is happening in matters that seriously affect it,

are basic psychological needs not to be denied in a democratic system.

Finally, by way of summary, the panel reviewed the relative power wielded by the five actors on national security policy. The President remains the central figure in policy formulation and he, with his personal advisers, will have the strongest effect on its outcome. The Executive Branch departments and agencies have a moderate influence and considerable potential, and could perhaps provide the avenue for improvements in dealing with long-range issues. Individual pressure groups can and do exert a strong and tightly-focused effect on policy, especially as they act on all the other participants in the process, but usually on only a narrow front. Congress and public opinion (under which rubric the media are included) possess gross tools or powers which, although of lesser influence than the other actors on a day-to-day basis, can cause radical changes and departures in policy, when they are aroused to do so by real or perceived abuse of power by the other actors.

Historical Perspectives

Professor Robert S. Wood
University of Virginia

In explanation of the forces motivating the drafters of the Constitution of the United States, James Madison wrote:

> *To secure the public good and private rights against the danger of (an overbearing majority), and at the same time to preserve the spirit and form of popular government is then the great object to which our inquiries are directed....*[1] *It is a melancholy reflection that liberty should be equally exposed to danger whether the government have too much or too little power, and that the line which divides these extremes should be so inaccurately defined by experience.*[2]

In effect, Madison conceived the great constitutive mission as the construction of a *democratic* form of government so organized as to be both solicitous of *individual rights* and *stable and competent* in operation. The formula by which this was to be accomplished was the twin principles of the separation of powers doctrine and the concept of checks and balances.

Madison defined tyranny as the concentration of power. As he observed in *The Federalist Papers*, number 47:

> *The accumulation of all powers, legislative, executive, and judiciary, in the same hands, whether of one, a few, or many, and whether hereditary, self-appointed, or elective, may justly be pronounced the very definition of tyranny.*[3]

The powers of government can thus be distinguished along functional lines — *i.e.*, legislative, executive, and judiciary — and should be divided into three branches of government. So divided, institutional jealousies and personal ambition will so operate as to forestall dangerous concentrations of power. Hence, as Madison wrote, "...the greatest security against a gradual concentration of the several powers in the same department consists in giving to those who administer each department the necessary constitutional means and personal motives to resist encroachment of the other."[4] Thus was asserted what M. J. C. Vile called the "pure doctrine of separation of powers."

> *A "pure doctrine" of the separation of powers might be formulated in the following way: It is essential for the establishment and maintenance of political liberty that the government be divided into three branches or departments, the legislative, the executive, and the judiciary. To each of these three branches, there is a corresponding identifiable function of government, legislative, executive, or judicial. Each branch of the government must be confined to the exercise of its own function and not allowed to encroach upon the functions of the other branches. Furthermore, the persons who compose these three agencies of government must be kept separate and distinct, no individual being allowed to be at the same time a member of more than one branch. In this way each of the branches will be a check to the others and no single group of people will be able to control the machinery of the State.*[5]

It was the conjunction of these ideas in the constitutional framework which was to provide a democratic government both *efficient* and *protective of individual liberties.** The Constitution thus embodies the American version of limited government. The critical question for any inquiry into national security policy is whether or not this constitutional formula was to be applied to the conduct of foreign affairs as it was to domestic policymaking.

Madison and the other founders did not, however, believe that a strict separation of powers would prove either efficient or adequate to prevent an abuse of power. The doctrine was therefore complemented by checks and balances. In effect, the separation of powers did not require the branches of government, in Madison's words, to "be wholly unconnected with each other" and indeed he argued that "unless these departments be so far connected and blended as to give each a constitutional control over the others, the degree of separation which the maximum requires, as essential to a free government, can never in practice be duly maintained."[6] In effect, the constitutional system was so devised as to require the cooperation of the separate branches if government were to function at all.

* emphasis supplied

As Mr. Vile explained:

The pure doctrine as we have described it embodies what might be called a "negative" approach to the checking of the power of the agencies of government. The mere existence of several autonomous decision-taking bodies with specific functions is considered to be a sufficient brake upon the concentration of power. Nothing more is needed. They do not actively exercise checks upon each other, for to do so would be to "interfere" in the functions of another branch. However, the theory does not indicate how an agency, or the group of persons who wields its authority, are to be restrained if they do attempt to exercise power improperly by encroaching upon the functions of another branch. The inadequacy of the controls which this negative approach to the checking of arbitrary rules provides, leads on to the adoption of other ideas to complement the doctrine of the separation of powers and to modify it.

The most important of these modifications lies in the amalgamation of the doctrine with the theory of mixed government, or with its later form, the theory of checks and balances.... From an analytical point of view, the main consideration is that these theories were used to import the idea of a set of positive checks to the exercise of power into the doctrine of the separation of powers. That is to say that each branch was given the power to exercise a degree of direct control over the others by authorizing it to play a part, although only a limited part, in the exercise of the other's functions. Thus, the executive branch was given a veto power over legislation, or the legislative branch was given the power of impeachment. The important point is that this power to "interfere" was only a limited one, so that the basic idea of a division of functions remained, modified by the view that each of the branches could exercise some authority in the field of all three functions. This is the amalgam of the doctrine of separation of powers with the theory of checks and balances which formed the basis of the United States Constitution.[7]

Foreign Policy Prerogatives, Separation of Powers, and Executive Privilege: The "Classical" View

It is interesting to note that John Locke, another great contributor to the notion of limited government and one who exerted important influence on the thinking of the founders, did not place foreign policy power under the same limitations as other exercises of government authority. Locke, unlike the Founders, defined institutional limitations almost exclusively in terms of restrictions upon executive power — but, at the same time, he did not extend these restrictions to the executive's exercise of power in external affairs. Indeed, he referred to this latter assertion of executive authority by a special term, "federative" power.[8]

In his essay, *On Civil Government,* Locke argued that whereas government should be limited and controlled by the people with respect to domestic policies, the nature of external affairs was such that government must be sovereign and capable of speaking with one voice. Locke's argument may be related to the general tradition of "reason of state" — that is, that the security of the state is fundamental and undergirds whatever constitutional order may be established. Protection of the state and its external position is thus extra-constitutional and resides in that authority most able to mobilize forces and conduct a unified policy, the executive.

In the United Kingdom, this power was designated as "the King's prerogative" under which Blackstone's *Commentaries* listed "...The entire range of powers relating to war and peace, to diplomacy and the making of treaties, and to military command...."[9] Arthur Bestor thus describes Blackstone's position:

At the outset, Blackstone recognizes two different sources for the authority of the chief executive in the domain of foreign relations. Vis-a-vis other nations, the King "is the delegate or representative of his people." Therefore, the handling of all aspects of the "nation's intercourse with foreign nations" is an executive prerogative. The King is also "the generalissimo, or the first in military command, within the Kingdom," and this fact places in executive hands the control of a variety of matters relating to military security.... One of the variety of matters relating to military security is the "prerogatives to make treaties, leagues, and alliances with foreign states and princes." The next is "the sole prerogative of making war and peace."[10]

Those partisans of executive power in foreign affairs in the continuing debate over presidential prerogatives tend to emphasize both the general perspective of Locke and Blackstone and the near absolute character of the separation of powers doctrine, at least in the area of external policy.

Even Alexander Hamilton, who argued in the *Federalist Papers,* number 69, that the President's powers under the constitution were far inferior to those of the King of England, later asserted that authority over foreign relations was *per se* an executive function and that Congress was limited only to such authority as was specifically enumerated in the Constitution.[11] In practice, many implied powers flowed from the executive authority in foreign affairs whereas congressional power should be seen restrictively.

Under this line of reasoning, foreign policy is "executive" in nature and the presumption of authority

therefore should always be on the side of the President. As Justice Sutherland argued in *United States v. Curtiss-Wright Export Corporation* (1936): "In this vast external realm, with its important, complicated, delicate and manifold problems, the President alone has the power to speak or to listen as a representative of the nation."[12] And Senator J. William Fulbright supported in 1961 a near total presidential authority in the use of force: "...We have hobbled the President by too niggardly a grant of power... As Commander-in-Chief of the armed forces, the President has full responsibility, which cannot be shared, for military decisions in a world in which the difference between safety and cataclysm can be a matter of hours or even minutes."[13]

If the President possesses extensive prerogatives in the area of national security, then so too do many departments and subordinates acting under his general direction. An invocation of national security is thus a political question not subject to judicial interpretation or resolution under constitutional norms.

Moreover, this range of privileged presidential power is also justified on the general grounds of the separation of powers doctrine — that is, presidential discretion in the area of his executive functions is complete, subject only to the grossest of legislative discipline, *i.e.,* cutting off appropriations or impeachment. In effect, in carrying out an executive function, as long as they are not *clearly** criminal, deliberation and decisionmaking within the executive branch are privileged.

This assertion of a constitutional basis for executive privilege was the heart of Attorney General Richard Kleindienst's testimony on April 10, 1973, before a joint session of three subcommittees of the Senate's Government Operations and Judiciary Committee:

> *The separation of powers doctrine gives the President the constitutional authority...in his discretion to withhold certain documents or information in his possession or in possession of the executive branch from compulsory process of the legislative or judicial branch of the Government, if he believes disclosure would impair the proper exercise of his constitutional functions.*[14]

Earlier, President Eisenhower's Attorney General, William Rogers, later Secretary of State under Richard Nixon, also argued that:

> *By the Constitution, the President is invested with certain political powers. He may use his own discretion in executing these powers. He is accountable only to his country in his political character, and to his own conscience... Questions which the Constitution and laws leave to the Executive, or which are in their nature political, are not for the Courts to decide, and there is no power in the Courts to control the President's discretion or decision, with respect to such questions.*[15]

On this basis, Attorney General Rogers stated the privilege of the executive to withhold information from Congress in the following areas:

- Military and diplomatic secrets and foreign affairs;
- Information made confidential by statute;
- Investigations relating to pending litigation, investigative files, and reports;
- Information relating to internal government affairs privileged from disclosure in the public interest; and
- Records incidental to the making of policy, including interdepartmental memoranda, advisory opinions, recommendations of subordinates and informal working papers.[16]

In *United States v. Nixon,* 418 U.S. (1974), the court ruled that President Nixon could not invoke executive privilege to withhold from a prosecutor evidence in criminal proceedings. The issue did not concern a congressional request for information. However, the fact that the court did make a determination would tend to indicate that, in the court's view, executive privilege is not plenary nor entirely discretionary. At the same time, Chief Justice Burger did uphold the notion of executive privilege as rooted in the separation of powers doctrine:

> *The privilege can be said to derive from the supremacy of each branch within its own assigned areas of constitutional duties. Certain powers and privileges flow from the nature of enumerated powers; the protection of the confidentiality of Presidential communications has similar constitutional underpinnings.*[17]

Moreover, the Court did maintain that presidential assertions of privilege in order to protect matters relating to national security should be given the "utmost deference."[18]

Although the executive privilege asserted by Kleindienst and Rogers relates specifically to the transmission of information, both the substantive claims

*Emphasis supplied.

and constitutional arguments constitute a broad discretionary authority under the separation of powers doctrine. Coupled with an assertion of the peculiarly "executive" nature of foreign affairs, these arguments give enormous scope to the President's prerogatives in national security policy.

Although there is no question that there have been abundant arguments throughout history for broad presidential prerogatives in foreign affairs, the original question remains: What is the exact pattern of authority established by the Constitution and, assuming the language of that document is not necessarily unambiguous, what was the intent of the framers?

Foreign Policy Powers: Constitutional Language and Framer's Intent

Article I, Section 8, of the Constitution explicitly grants to Congress the power to "provide for the common Defence"; "regulate Commerce with foreign Nations"; "define and punish Piracies and Felonies committed on the high seas and Offences against the Law of Nations"; "declare War, grant letters of marque and reprisal, and make rules concerning captures on land and water"; "raise and support Armies"; "provide and maintain a Navy"; "make Rules for Government and Regulation of the land and naval forces"; "provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrection and repel Invasions"; "provide for organizing, arming, and disciplining the Militia, and for governing such Part of them as may be employed in the service of the United States"; and to "make all laws which shall be necessary for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof."[19]

If Article I, Section 8, grants specific authority, Article II, Section 2, states presidential authority not in terms of function but of office: "The President shall be commander in chief of the army and navy of the United States, and of the militia of the several states, when called into the actual service of the United States."[20] Partisans of presidential power assert that authority in external affairs, particularly war powers, not specifically delegated elsewhere, inhere in the executive office of the President. On the other hand, advocates of Congressional authority argue that the specific grants of authority in Article I, especially the power "to declare war," provide Congress with an amplitude of power, including the right to authorize war. Indeed, in 1793, none other than James Madison defined external power, and most specifically war making, not as being executive but legislative in character: "The power to declare war...including the power of judging the causes of war, is fully and exclusively vested in the Legislature, that the executive has no right in any case, to decide the question whether there is, or is not cause for declaring war."[21]

If one examines the record of the debates of the Constitutional Convention, it in fact becomes rather clear that the framers, unlike John Locke, did not treat the exercise of power externally as something apart from the general constitutional formula. There was indeed an attempt to organize a unified foreign policy represented by the executive branch but in coordination with Congress. As in other areas, both the separation of powers and checks and balances were to govern the conduct of foreign affairs.

Much of the debate concerning the relative authority of President and Congress centered on the power to declare war. The original draft empowered Congress "to make war," but it was felt that this wording was too restrictive on the Executive in case of sudden attacks. Moreover, it was generally agreed that the normal conduct of war, once initiated, was an executive function. Nonetheless, there appeared to be general agreement that the determination of war was normally a legislative function.[22] Hence, Raoul Berger concluded that the Constitution "...conferred virtually all of war making powers upon Congress, leaving the President only the power 'to repel sudden attack' on the United States."[23] It would seem that Madison's assessment of the respective powers of President and Congress was accurate.

But, if Madison was correct as to the general consensus at the Constitutional Convention, many have argued that he was wrong in terms of the historical evolution which in the long haul favored presidential authority. Eugene Rostow criticizes those scholars who seek to delimit foreign policy authority on the basis of the Constitutional Convention. He argues that they too readily

> *...dismiss the fact that the men who made the Constitution had quite another view of its imperatives when they became Presidents, Senators, Congressmen, and Secretaries of State. The words and conduct of the Founding Fathers in office hardly support the simplified and unworldly models we are asked to accept as embodiments of the only True Faith.*[24]

Foreign Policy Powers: The Historical Evolution

As early as 1793 the nation was torn by a presidential assertion of foreign policy authority. In response to Washington's declaration of neutrality between France and England, Hamilton writing as "Pacificus" defended the executive right to determine war whereas Madison writing as "Helvidius" upheld a legislative right in this area. As it turned out, Washington's position prevailed, as Congress enacted a neutrality act on June 5, 1794.[25]

In 1795, by the Militia Act Congress granted to the President authority to mobilize and command the

state militia "...whenever the United States shall be invaded, or be in imminent danger of invasion from any foreign nation or Indian tribe."[26] Both in this case and that of the war between Britain and France, one could argue that Congress did in fact assert its legislative authority. But, at the same time, a process of sustaining prior presidential actions and granting him broad discretionary authority was begun.

This expanding view of presidential power was subsequently sustained by two Supreme Court decisions. In *Martin* v. *Mott* (1827), Justice Story argued "The authority to decide whether the exigency [requiring the use of militia under the Militia Act of 1795] has arisen belongs exclusively to the President, and his decision is conclusive upon all other persons."[27] And in *Luther* v. *Borden* (1849), the court in effect declared the question as to whether an emergency sufficient to require the exercise of force existed a "political question" and beyond the competence of the Court. "It is said that the power in the President is dangerous to liberty, and may be abused. All power may be abused if placed in unworthy hands. But it would be difficult, we think, to point out any other hands in which this power would be more safe, and at the same time equally effectual."[28]

American history is replete with instances of assertions of war-making power by the President or his subordinates without legislative authorization or at times even subsequent formal approval. A notable early example in 1818 was General Andrew Jackson's foray on President James Monroe's orders into Spanish Florida in pursuit of renegade Indians and the subsequent attacks by Jackson on Spanish forts and Indians alike as well as the summary execution of two British citizens. And in the Mexican-American War one can certainly argue that President Polk presented the Congress with a *fait accompli* virtually compelling a Congressional declaration of War. As William Howard Taft observed, "...Congress has the power to declare war, but with the army and navy, the President can take action so as to involve the country in war and to leave Congress no option but to declare it or recognize its existence."[29] And indeed, despite the dominance of legislative authority between Jefferson and Lincoln, one study indicates that over 60 reported military hostilities occurred without explicit Congressional authorization or a declaration of war.[30]

It is generally agreed that President Abraham Lincoln was the principal architect of the modern expansion of the powers of the Commander-in-Chief — ironical in view of Congressman Lincoln's dissent from Polk's action in Mexico.[31] By virtue of the Commander-in-Chief clause and the clause which makes it the duty of the President "to take care that the laws be faithfully executed," Lincoln without prior consent of Congress suspended *habeas corpus,* ordered money advanced from the treasury without legislative appropriation, expanded the armed forces, ordered summary arrests and confiscation of property, submitted civilians to military tribunals, and ordered a blockade of southern ports.

In the twentieth century, President William McKinley acted solely on his authority as Commander-in-Chief when he dispatched a naval force and 5,000 land forces to participate in the international expedition to suppress the Boxer Rebellion in China. Theodore Roosevelt explicitly embraced an expansive view of the executive power in foreign affairs: "The biggest matters (of my administration), such as the Portsmouth peace, the acquisition of Panama, and sending the fleet around the world, I managed without consultation with anyone; for when a matter is of capital importance, it is well to have it handled by one man only."[33] Subsequent to raids by Pancho Villa into New Mexico, Woodrow Wilson authorized a punitive expedition into Mexico without formal congressional sanction. Similarly, he committed forces in North Russia and Siberia following the Bolshevik Revolution in 1917. Although there was substantial opposition in Congress and two resolutions were introduced with the intent of halting the expeditions, no Congressional action was taken.

Although these initiatives are classified as domestic and although the court did later invalidate certain of Lincoln's activities (*i.e.,* suspension of *habeas corpus,* martial law), these actions together are generally indicative of the expansion of executive power during crises and tend to sustain the notion that the power to protect the fundamental security and integrity of the state is extra-constitutional. Moreover, in the *Prize Cases* (1862), the Court reaffirmed the "political question" notion of *Luther* v. *Borden* and asserted the primacy of the President in the determination of war and peace:

> *Whether the President, in fulfilling his duties, as Commander-in-Chief, in suppressing an insurrection, had met with such armed resistance...as will compel him to accord to them the character of belligerents, is a question to be decided by him, and this Court must be governed by the decision and acts of the political department to which this power was entrusted.*[32]

After the Civil War, the most significant increases in presidential power occurred during the two World Wars. After a refusal by Congress in 1917 to allow him to arm merchant ships bound for Europe, President Wilson undertook the action on his own authority and thus moved the United States closer to war. Similarly, President Franklin D. Roosevelt without Congressional authorization exchanged 50 American destroyers for the lease of British bases, placed Greenland under U.S. control and Iceland under American protection, occupied Dutch Guinea, and in

1941 issued the famous "shoot-on-sight" order to the Navy: "when you see a rattlesnake poised to strike, you do not wait until he has struck before you crush him. The Nazi submarines and raiders are the rattlesnakes of the Atlantic... They are a challenge to our sovereignty."[34] And, of course, the apparent vindication by the Japanese at Pearl Harbor of Roosevelt's prewar actions in the face of hostile Congressional criticism strengthened the President's assertion of presidential prerogatives during the war. As Arthur Schlesinger, Jr., explained: "The grand revival of the presidential prerogative after Pearl Harbor must be understood as a direct reaction to what happened when Congress tried to seize the guiding reins of foreign policy in the years 1919 to 1939."[35]

Indeed, President Harry Truman's ability to commit troops to Korea and the decision to expand forces in NATO, both without Congressional approval, probably stemmed in part from the memories of the interwar period. And, it is a fact that notable instances of Congressional assertions in foreign policy, *e.g.,* The War of 1812, The Spanish-American War, and the interwar period, have fared rather badly in the judgment of historians. The French commentator, Raymon Aron, well expressed in 1974 the attitude of those who unfavorably contrast presidential and congressional initiatives in foreign affairs:

> *...it is on Richard Nixon and Henry Kissinger that a European pins his hopes for a foreign policy governed by reason. The elected representatives of the American nation are swayed today by economic interests, both commercial and monetary, since public opinion does not cry out in fear of an enemy or call for a crusade against evil. It was in a somewhat similar period that Congress voted the Hawley-Smoot protective tariff. It is to the presidency rather than the Senate that Europeans look for an equitable policy.*[36]

What is remarkable about this statement is that it was made in full cognizance of the Watergate scandal. So searing was the experience of the interwar period and so substantial was the foreign policy prestige of the presidency that the constitutional qualms that Senator Robert Taft expressed in the early fifties were still dismissed out of hand by many foreign and domestic commentators in the early nineteen seventies.

If in political practice a wide amplitude of executive power in foreign affairs has been successfully asserted, so the Supreme Court on those rare occasions when it pronounces on the subject at all has tended to sustain presidential prerogatives. This was true not only of the early *United States* v. *Curtiss-Wright Corporation* but the *Youngstown Sheet and Tube Company* v. *Sawyer* (1952) case. Although Truman's seizure of the steel mills was held to be unconstitutional, the decision reemphasized the President's external prerogatives. As Justice Jackson states:

> *We should not use this occasion to circumscribe, much less to contract, the lawful role of the President as Commander-in-Chief. I should indulge the widest latitude on interpretation to sustain his exclusive function to command the instruments of national force, at least when turned against the outside world for the security of our society...*[37]

And, of course, the Court in *United States* v. *Nixon* spoke of "utmost deference" to the President's external authority.

It should be clear that neither the Constitution nor the intent of the framers definitively resolved the respective authority of the branches of government in the conduct of foreign affairs. It is equally true that the President has tended to assert successfully the widest prerogatives in the long term. On the other hand, the Congress has tended to reassert itself after most strong Presidents and the relative balance is always subject to dispute. Moreover, one might argue that the framers of the Constitution intended this tension and shifting weight as a result of their extension of the principle of checks and balances to the conduct of foreign affairs. Indeed, although the experience from the end of World War II until the early seventies tended to strengthen presidential prerogatives, one can discern shifts within Congressional-Presidential relationships and attempts at major restructuring in the mid-seventies.

Foreign Policy Powers: The Experience Since World War II

It should be noted that the extension of presidential prerogatives is not limited to the conduct of foreign affairs. The general tendency in modern times and in a wide diversity of policies is to strengthen the executive and administrative at the expense of the legislative. However stark and apparently exaggerated it seems, Richard Nixon's recent statement in fact represents a general tendency:

> *The point is: that when an agency is asked by a President or anybody else to do something that it has a responsibility to do, that's not illegal for them to do it or for it to be ordered, even if the motivation is political...*[38]

Indeed, Woodrow Wilson early in the century philosophically defended the widest latitude for presidential authority and explicitly rejected the Madisonian amalgam of separation of powers and checks and balance.[39] And in practice modern presidents have in one degree or another behaved in line with Wilson's dictum.

Wilson saw the Constitution as a transitory document suitable to a nation characterized by sharp diversity. With the emergence of a harmonious national community wrought by technology, war, and education, the structured conflict of the Constitution was no longer necessary and was in fact harmful. Indeed, from Wilson's perspective, although the nation had from 1787 onward a Constitution, it did not have a constitutional system. He defined constitutionalism not in terms of limitations on governmental power but in terms of "common understandings, common interests, common impulses, common habits" which allow the government extensive power to realize community objectives:[40]

> *Evidently, if a constitutional government is a government conducted on the basis of a definite understanding between those who administer it and those who obey it, there can be no constitutional governnment unless there be a community to sustain and develop it, — unless the nation whose instrument it is, is conscious of common interests and can form common purposes. A people not conscious of any unity, inorganic, unthoughtful, without concert of action, can manifestly neither form nor sustain a constitutional system. The lethargy of unawakened consciousness is upon them, the helplessness of unformed purpose. They can form no common judgment; they can conceive no common end; they can contrive no common measures: nothing but a community can have a constitutional form of government, and if a nation has not become a community, it cannot have that sort of policy.*[41]

Wilson saw the wielding of the House of Representatives into an "organic" unit under disciplined leadership and the development of strong parties as reflective of an emergent harmonious community. By contrast, he saw the Senate as regressive, more individualistic, and less representative — a holdover from the past. Senators reflect a particular community and not a national one. But it is the President who preeminently represents this national community and who, supported by a strong party system, will overcome the divisiveness of the federal system of representation and the hindrances of the eighteenth century constitution. Indeed, in the execution of the popular will the President should be allowed to make of the office of the President "anything he has the sagacity and force to make it" unfettered by legal inhibitions.[42] Indeed, the power of the presidency is extra-legal: "His executive powers are in commission, while his political powers more and more center and accumulate within him and are in their very nature personal and inalienable."[43]

Wilson showed a remarkable distrust for legal restrictions: "The gauge of excellence is not the law under which officers act, but the conscience and intelligence with which they apply it, if they apply it at all."[44] Presidential power should be seen less in formal than personal terms: "The President is at liberty, both in law and conscience, to be as big a man as he can. His capacity will set the limit,"[45] and presumably not the formal Constitution, for "the personal force of the President is perfectly constitutional to any extent to which he chooses to exercise it, and it is clear by the logic of our constitutional practice that he has become alike the leader of his party and the leader of the nation."[46] The future presidency, in Wilson's view, would — less in terms of formal power and more in terms of personal power — represent the spirit of the national community:

> *[We] can safely predict that as the multitude of the President's duties increases, as it must with the growth and widening activities of the nation itself, the incumbents of the great office will more and more come to feel that they are administering it in its truest purpose and with greatest effect by regarding themselves as less and less executive officers and more and more directors of affairs and leaders of the nation, — men of counsel and of the sort of action that makes for enlightenment.*[47]

Unquestionably the Wilsonian view of the presidency came to dominate the perspective of popular and academic commentators alike. Heavy emphasis on presidential prerogatives generally would almost perforce be matched by even greater support for executive power in foreign affairs, given the classical view of the extra-constitutional nature of this authority and the presumed exigences of the nuclear age. By the same token, therefore, shifts in the Congressional-Presidential balance and increasing defenses of legislative prerogatives in foreign affairs reflect not only assessments of the structure of authority and decisionmaking in the area of foreign policy, but often represent a general debate on the nature and power of the presidency. This is certainly true of the current period. In any case, any evaluation of legislative-executive relations in the area of foreign affairs since World War II should take into account the broader question of the constitutional and political balance generally.

Frans R. Bax argues that there have been five successive phases in legislative-executive relations in the area of foreign affairs since World War II: a period of *accommodation* from the presentation of the UNRAA program to Congress in 1943 until 1950-51; a period of *antagonism* from 1951 until 1955 dominated by both partisan and institutional rivalries; a period of *acquiescence* beginning in 1955 and lasting for a decade in which Congress tended to legitimize presidential actions without participating as an active partner or assuming responsibility; a period of *ambiguity* beginning in 1966 and ending with the invasion of Cambodia in the spring of 1970 and characterized by

growing doubts about the substance of Administration policy and concern over the passive role of Congress in the formulation of foreign policy; and a period of *acrimony* initiated at the time of the Cambodian action in which Congress moved to challenge not only the specific elements of U.S. policy in Vietnam and elsewhere but to alter the manner in which national security policy was developed and implemented by asserting a more independent role for Congress in the process.[48] Although Congressional-Executive relations are always somewhat fluid, Professor Bax's categorization appears to be a sufficiently accurate organization of the time.

The important feature of the early period of accommodation was the pattern of close consultation which grew out of Congressional insistence that the UNRAA program not be accepted by executive agreement but after submission to Congress. The key figure in the development of this collaboration was a Republican Senator, Arthur Vandenberg, and the period saw the approval of such complex or far-reaching commitments as the Marshall Plan and the NATO treaty.

With the passing of Vandenberg, however, the "loss" of China, and the mounting costs of the Korean War, Congressional-Presidential relations entered a period of acrimonious charges and counter charges symbolized by the Bricker Amendment, which would have clearly ensured Congressional approval of all international agreements concluded by the President. Moreover, the decision of the Truman administration in 1951 to increase American forces in Europe by four divisions without prior Congressional authorization triggered strong Congressional opposition headed by Senator Robert Taft who argued:

> *The President has no power to agree to send American troops to fight in Europe in a war between the members of the Atlantic Pact and Soviet Russia. Without authority he involved us in the Korean War. Without authority he apparently is now attempting to adopt a similar policy in Europe.*[49]

Although the Bricker Amendment failed to receive the necessary two-thirds majority, it was only by a single vote, and the concerns raised by Taft were widely shared. Moreover, during this period, Senator Joseph McCarthy's influence cast a pall over Executive-Legislative relations.

The election of Dwight Eisenhower and the reduced influence of McCarthy appeared to signal a return to accommodation; but, after the Democrats regained control of Congress in 1955, consultations between the two branches declined and Congress, as Bax argues, tended to legitimize rather than actively participate in the formulation of national security policy. It was only the length, cost, and inconclusiveness of the Vietnam War which gave rise first to a period of ambiguity and then acrimony in Executive-Legislative relations. But unlike the earlier period of antagonism, Congress successfully moved by legislative acts to curb the power of the President, although the durability of such actions may still be a subject of some debate.

In June 1969, by a 76 to 19 vote, the Senate voted the "National Commitments Resolution" which read:

> *Whereas accurate definition of the term "national commitment" in recent years has become obscured: Now, therefore, be it Resolved, that it is the sense of the Senate that a national commitment by the United States to a foreign power necessarily and exclusively results from affirmative action taken by the executive and legislative branches of the United States Government through means of treaty, convention, or other legislative instrumentality specifically intended to give effect to such a commitment.*[50]

The Cambodian Invasion of 1970 brought forth a plethora of amendments to financial authorization or appropriation bills to limit the President's power to maintain or employ combat forces in Indochina. Finally in 1971, an amendment to the Special Foreign Assistance Act stipulated that funds could neither be authorized nor appropriated "to finance the introduction of United States ground combat troops into Cambodia, or to provide United States advisors to and for Cambodian military forces in Cambodia."[51] In August 1973 the President was forbidden to employ U.S. forces in Indochina in the future. In other areas, such as Cyprus, Angola, and Soviet immigration, Congress quickly moved to restrain or control the Administration's conduct of foreign policy.

Aside from substantive disagreements between the Executive and Legislative branches, Congress moved to assert its authority in the formulation of foreign policy through legislative act and institutional innovation. Basically, the Congress acted in two areas: (1) *war making power* and (2) *intelligence and information.*

Alexis de Tocqueville in his *Democracy in America* noted that American tendency to resolve substantive differences through procedural initiatives and to translate political into legal issues.[52] Given the Constitutional framework within which national security policy has developed, it was nearly inevitable that the substantive disagreements and institutional rivalries of the early seventies would be cast in legal and procedural terms. And the whole Watergate episode merged with the foreign policy questions to raise the issue to the level of a general Constitutional confrontation. The passage of the *War Powers Resolution* of 1973 symbolized this confrontation as had few other actions.

Quite simply, the War Powers Act required consultation with the Congress on the part of the President prior to the introduction of military forces into actual or potential conflict. It further required a report in justification of such action within 48 hours of deployment. In an emergency the President might deploy combat forces without authorization but such forces must be withdrawn within 60 days unless Congress gives its formal assent. There may be a single 30-day extension if the President certifies in writing that the extension is essential to the protection of U.S. forces. During this 90-day period and presumably beyond, Congress may recall all troops by the passage by a simple majority of both houses of a concurrent resolution which would not be subject to a Presidential veto. Congressional power is defined broadly whereas Presidential powers to introduce forces "into hostilities, or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, are exercised only pursuant to (1) a declaration of war, (2) specific statutory authorization, or (3) a national emergency created by attack upon the United States, its territories or possessions, or its armed forces."[53]

In respect to information and intelligence operations, the Subcommittee on United States Security Agreements and Commitments Abroad reported in 1970 a number of important commitments undertaken abroad without the knowledge or participation of Congress. Congress subsequently passed a bill requiring the prompt reporting of executive agreements and many items of regular legislation established reporting requirements. Representative William S. Moorhead, Senators Mike Gravel, Jacob Javits, and Edmund Muskie all have introduced various bills aimed at the establishment of legislative committees empowered to establish and regulate government classification systems.[54] And, most importantly, a Senate Select Committee on Intelligence was established in 1976.

This latter committee stemmed from the determination of former Senate Majority Leader Mike Mansfield to establish effective congressional oversight over U.S. foreign intelligence activities. The experience of Vietnam, the Watergate investigations, and various journalistic exposes all prompted demands for official investigations — the result of which were the Rockefeller Commission in the Executive branch, the Pike Committee in the House of Representatives, and the Church Committee in the Senate. It was the work of the latter which eventuated in the Senate Select Committee. The charter of the committee made it privy to essentially all information about U.S. intelligence activities — a radical break with the past.[55]

It is thus clear that the period of acrimony has given rise to important procedural and institutional developments. The important question concerns the future relation of the executive and legislative branches in the area of foreign affairs. Obviously, continuing acrimony would serve neither the Congress nor the nation. Nor is it possible for Congress to act as chief representative, negotiator, or Commander-in-Chief for the nation. Good faith on the part of both branches and sufficient deference on the part of Congress to allow some executive flexibility seem essential for the effective conduct of foreign affairs. In effect, if the current restructuring of relations between Congress and President allows a return to accommodation and partnership, however competitive the relationship may at times be, then the nation may be well served. As Wolfram Hanrieder once observed, an effective foreign policy must be "compatible" with the challenges and opportunities of the external environment and command a broad internal "consensus."[56] It is not always easy to reconcile these demands but there appears to be no alternative than to attempt it.

If American society is beset in the seventies with suspicions concerning the general effectiveness of government, so many commentators have come to doubt the omnicompetence of the President or the uniqueness of his representation of the national community. The attempt to render Congress a more responsible and active partner in the development of national security policy is thus part of a general movement in political thought. To some degree, in foreign affairs, we appear to be moving away from Woodrow Wilson and back toward James Madison. Whether this is but a slight detour away from a continuing national trend remains to be seen.

ENDNOTES

1. *The Federalist Papers*, No. 10.

2. James Madison to Thomas Jefferson, October 17, 1788, in *Writings, V*, p. 272.

3. *The Federalist Papers*, No. 47.

4. *Ibid.*

5. M. J. C. Vile, *Constitutionalism and the Separation of Powers* (1967), p. 13.

6. Cited in Arthur Bestor, "Separation of Powers in the Domain of Foreign Affairs: The Original Intent of the Constitution Historically Examined," *Seton Hall Law Review*, Vol. 5, Spring, 1974, p. 536.

7. Vile, *op. cit.*, p. 18.

8. John Locke, "On Civil Government," in Edwin A. Burtt, editor, *The English Philosophers to Mill* (1939), pp. 462-463.

9. Bestor, *op cit.*, p. 530.

10. *Ibid.*, pp. 532-533.

11. See *The Works of Alexander Hamilton IV*, H. Lodge, editor (1906), pp. 437-444.

12. 299 U.S. (1936), 319.

13. Fulbright, "American Foreign Policy in the Twentieth Century Under an 18th Century Constitution," *Cornell Law Quarterly* 47 (1961), p. 50.

14. U.S. Congress, Senate, Committees on Government Operations and The Judiciary, *Executive Privilege, Secrecy in Government, Freedom of Information*, Hearings before the subcommittees on Intergovernmental Relations, Separation of Powers, and Administrative Practice and Procedure, Senate, Vol. I, 93d Congress, 1st session, 1973. Cited by James Hamilton, *The Power to Probe: A Study of Congressional Investigations* (1976), p. 157.

15. U.S. Congress, Senate, "The Power of the President to Withhold Information from Congress," Memoranda of the Attorney General; compiled by the Subcommittee on Constitutional Rights, of the Committee on the Judiciary, U.S. Senate, 85th Congress, 2d session, 1958, p. 24.

16. N. Dorsen and J. H. F. Shattuck, "Executive Privilege, The Congress and The Courts," reprinted in U.S. Congress, House of Representatives, *Availability of Information to Congress*, Hearings before a subcommittee of the Committee on Government Operations, House of Representatives, 93d Congress, 1st session, 1973, p. 279.

17. 418 U.S. (1974), pp. 705-706.

18. *Ibid.*, pp. 710-711.

19. U.S. Constitution, Article I, Section 8.

20. *Ibid.*, Article II, Section 2.

21. *The Writings of James Madison VI*, G. Hunt, editor (1906), p. 174.

22. *The Records of The Federal Convention II*, M. Farrand, editor (rev. ed., 1937), p. 319.

23. R. Berger, "War Making by The President," *University of Pennsylvania Law Review* 212 (1972), p. 82.

24. E. Rostow, "Great Cases Make Bad Laws: The War Powers Act," *Texas Law Review* 50 (1972), p. 841.

25. See E. Corwin, *The President: Office and Powers* (3d ed., 1948), p. 217.

26. Act of February 28, 1795, ch. 36, section 1, 1stat., p. 424.

27. 25 U.S., 12 Wheat. (1827), p. 30.

28. 48 U.S., 7 How., (1849), p. 44.

29. W. H. Taft, *The Presidency* (1916), p. 86.

30. Emerson, "War Powers Legislation," *West Virginia Law Review* 74 (1972), p. 92.

31. A. Lincoln, *Collected Works*, R. P. Basler, editor (1953), pp. 451-452.

32. 67 U.S., 2 Black, (1862), p. 670.

33. T. Roosevelt, *Letters*, E. Morrison, editor (1956), pp. 1497-1498.

34. *New York Times*, December 9, 1941, at 1, col. 1.

35. A. Schlesinger, Jr., *The Imperial Presidency* (1973), p. 99.

36. R. Aron, *The Imperial Republic* (1974), pp. X-XI.

37. 343 U.S. (1952), p. 645.

38. *Washington Post*, May 20, 1977, at A16, col. 5.

39. For an excellent discussion of Wilson's position, see S. A. Pearson, "The Crisis of American Constitutionalism" in Woodrow Wilson's "Constitutional Government: Community and the Prerequisites for Self-Government," unpublished manuscript, University of Virginia.

40. W. Wilson, *Constitutional Government in The United States* (1908), p. 46.

41. *Ibid.*, pp. 25-26.

42. *Ibid.*, p. 69.

43. *Ibid.*, p. 67.

44. *Ibid.*, p. 17.

45. *Ibid.*, p. 70.

46. *Ibid.*, p. 71-72.

47. *Ibid.*, p. 81.

48. F. R. Bax, "The Legislative-Executive Relationship in Foreign Policy: New Partnership or New Competition," *Orbis* 20 (1977), pp. 881-904.

49. 97 Congressional Record (1951), pp. 55-60.

50. U.S. Senate, Committee on Foreign Relations, *National Commitments*, Senate Report No. 129, 91st Congress, 1st session, 1969.

51. 84 Statutes (January 5, 1971), p. 1943.

52. A. de Tocqueville, *Democracy in America*, J. P. Mayer, editor (1967), p. 270.

53. Act of November 7, 1973, Pub. L. No. 93-148, 55 Stat, 555-560. For an excellent discussion of the War Powers Act, see J. C. Cruden, "The War Powers Act and National Security" (Unpublished M. A. thesis, University of Virginia, 1975).

54. For a thorough discussion of these initiatives, see J. S. Tomashoff, "Congressional Access to Foreign Policy Information Gathered by the Executive: A Necessary Concomitant for Effective Oversight" (Unpublished M. A. thesis, University of Virginia, 1977).

55. For an excellent discussion on The Select Committee, see E. P. Levine and S. A. Taylor, "U.S. Senate Oversight over the Intelligence Community: Power and Strategies," a paper prepared for presentation at the 18th Annual Convention of the International Studies Association, St. Louis, March 16-20, 1977.

56. W. Hanrieder, *West German Foreign Policy 1945-1963* (1967), pp. 1-10.

Inter-Sector Cooperation and Competition

Where Do We Go From Here?

Professor Adam Yarmolinsky
University of Massachusetts

The process of shaping national security policy for the United States in the best of all possible worlds ought to be a simple and straightforward one. We need only determine what should be our foreign policy objectives, to what extent those objectives can and should be accomplished through national security measures, and what national security resources should be applied to make these measures achievable and believable.

There are at least three difficulties with this formulation:

Foreign policy objectives can no longer be separately stated, except in the most general terms. Foreign policy is rather an aspect of every major national policy decision, and every foreign policy option must be examined in the light of its domestic policy consequences. Farm policy is domestic policy and it is foreign policy. Trade policy is foreign policy and it is domestic policy. Human rights issues reverberate in the domestic and the international arena.

National security measures can no longer be treated separately from other means of policy implementation. The United States is too much involved in the world, in too many complicated ways, for us to be able to say about any important problems, "This is a national security problem" or "This is not a national security problem." Just as there is a foreign policy aspect to almost every domestic policy decision, so there is a national security aspect to almost every foreign policy decision. Clearly, deterring nuclear attack depends on national security measures. But reducing the risk of nuclear proliferation is at least as much a function as energy policy and trade policy and development assistance policy, as it is of "national security policy" *per se.* Sorting out appropriate national security measures is like playing a game in which the rules (and even the players) are constantly changing.

As President Carter observed in his Notre Dame commencement address in May, "We can no longer separate the traditional issues of war and peace from the new global questions of justice, equity, and human rights."

National security resources are not created ex nihilo. We already have a 100-plus billion dollar military establishment, the largest single institution in American society today, in which *major new weapons systems take upwards of 10 years to develop,** from concept to deployment. Decisions about what national security resources should be developed are based on decisions about what national security policies should be pursued. But national security policy choices are also based on available national security resources, and the resource base changes only gradually — and in response to a variety of other influences as well as national security policy decisions: political, bureaucratic, and just plain inertial influences. Thus, policy decisions and resource decisions have almost as ambivalent a cause and effect relationship as the chicken and the egg.

Given these complexities, it is scarcely surprising that national security policy — like most public policy — changes slowly and incrementally, and is more nearly predictable on the basis of what national security policy has been, than on any other basis. After all, we do not yet have a coherent national energy policy, or a coherent national welfare policy, or even a coherent national tax policy.

Once a clear national consensus had developed on the political and moral necessity for U.S. withdrawal from Vietnam, it took more than 4 years for that withdrawal to be accomplished. Granted, the incumbent administration was at least partially paralyzed by the Watergate crisis during most of that period — but that is still a long time.

Lyndon Johnson observed in 1964 that, "There is no longer one Cold War." It has taken 12 years until Jimmy Carter could articulate effectively for the American people the proposition that while the Soviet Union remains our principal antagonist in the world arena, we can no longer organize our foreign policy around that *single* fact.

The nuclear triad — which is so central to the *theology* of nuclear deterrence — developed largely out of a series of historical accidents, fueled by interservice rivalry. But, the possiblity of abandoning any element of the triad in the short or even the middle run is very small — and for sound political reasons — unless we can do so by agreement with the Russians, which presents its own set of difficulties.

Not only does national security policy change slowly, but it has not been really very widely debated. What is surprising is how few genuine national debates we have had on national security issues over the past 30 years. Between the debate that led to our post-war commitment to our European allies, first through the Marshall Plan, and then through NATO, and the debate that led to our withdrawal from Vietnam, there was an emotional flare-up over who lost

* Emphasis supplied.

Communist China (as if it were ours to lose), a number of struggles within the military establishment over rival weapons systems, and some election-eve quarrels over the adequacy of our defenses. National security crises tend to draw the country together, as in the wake of the North Korean invasion or the Cuban missile crisis, but they do not seem to produce policy debates at the national level.

One can argue of course about what amounts to a national policy debate. Clearly, it is something more than a disagreement within the executive branch, even if the disagreement reaches the cabinet level. It ought to be something more than a partisan brawl in the Congress. It should probably exclude excitement generated by extremist groups on one side or another, provided the excitement is pretty well limited to those groups. A fair test of the genuineness of a national debate — although a difficult one to administer — might be the extent to which it engages the active interest of opinion leaders outside government, over a wide range of communities of interest.

By this test, perhaps the only real national debates over national security program and force structure were the 1968-69 ABM debate and, to a lesser extent, the 1961 civil defense debate; and the debate over the termination of the war in Vietnam, with its subsequent fallout in the debate over the war powers of the Executive. Significantly, all of these debates involved issues with an immediate domestic impact, in the location of ABM sites, in the construction of fallout shelters, and in the expenditure of American blood and treasure in South East Asia. A fourth debate seems to be shaping up on the export of nuclear power technology, particularly enrichment and reprocessing technology, and this debate too, if it develops, will have its roots in powerful domestic economic interests.

When one looks at these four examples, one can project that the frequency of national debates on national security issues is likely to increase, since those issues are increasingly involved with domestic matters directly affecting — either favorably or adversely — important interest groups in the United States, many of which are not elements of what is usually thought of as the military-industrial complex.

If we discovered in the sixties that the optimum national security could not be obtained by ignoring the costs of national defense — that calculating tradeoffs was the name of the game — we may be learning in the seventies that it is not a simple zero-sum game, that we cannot afford to think of the defense establishment as pitted against other interests in society. It is not just the inherent ambiguities and uncertainties of national security policy in a multipolar world that tend to depolarize disagreements over those issues within the domestic polity. It is also the fact that so many active interest groups are involved.

The issues are likely to be so complicated, moreover, that one cannot identify in advance which interest groups will be on which sides — and these issues are likely to have more than two sides. What is predictable is that defense industry — and the complex of interests that surrounds it — is likely to have a less dominant position among all the domestic interest groups — if only because there will be more of them with direct interests.

The energy issue, for example, is inextricably intertwined with national security, and it involves the energy industry, or rather industries, the automobile-industrial complex, consumers, environmentalists, etc. Technology transfer is an issue that sharply divides the military-industrial complex, and that involves other high-technology industries, where precedents may be set for defense industry. How we handle our grain reserves (or indeed how far we go to establish and maintain such reserves) is a question with all kinds of national security implications, but it is also an issue involving and affecting farmers, food processers, consumers and grain traders. The Law of the Sea Treaty, currently in negotiation, affects naval deployments, rights of innocent passage, and access to raw materials in the seabed that may become essential to national security. It also affects major extractive industries in the United States, and involves our relations with all the less developed countries, who have argued for a quite different regime to control those seabed resources.

Traditional national security issues are often presented in terms of oversimplified national security principles:

- The United States must be militarily strong.
- The United States must not be overextended.
- We cannot trust the Russians.
- We must stop the arms race.

Since most critical national security issues in fact involve a delicate balancing of competing technical considerations, how popular opinion divides on these issues tends to be a function of the ability of the protagonists on both sides to identify a specific issue with one general principle rather than another. Whether popular opinion tends to support the production of the B-1 Bomber or the size of the U.S. ground forces commitment to Europe can easily become a battle of slogans. By the same token, Presidents and members of the legislative branch may feel somewhat more free to decide these issues on the basis of their own judgments, satisfied that they can justify a close call either way to their constituencies, except where the specific interest of a particular defense industry or of the partisans of a domestic defense installation are involved.

To put this last point another way, in the resolution of traditional national security issues, there is not likely to be any very coherent center of countervailing pressure to offset the institutional pressures of the national security establishment. There is likely to be a systematic bias, therefore, towards bureaucratic solutions: preserving the status quo, expanding existing programs, and resisting major innovations. The expansionist tendency may then run up against overall budgetary constraints imposed by pressures on the entire federal budget (and by the fact that the defense budget has become one of the decreasing number of areas of "discretionary" spending), and the consequences of this encounter may be ill-advised budget cuts, based more on internal bureaucratic considerations than on considerations of national policy.

But the new kind of issues affect too many domestic interests that will not be turned off by slogans, because they are too much involved, and too sophisticated, as suggested in the examples above. Politics, in the broadest sense, can no longer stop at the water's edge, because the water's edge no longer marks a significant boundary in national affairs.

Add to these circumstances the general tendency to greater openness in discussions of public policy (a combination of a post-Watergate push and a Jimmy Carter pull) and the public demand for more and earlier explanations of what government is up to, and the result is likely to be a good deal more general discussion of issues involving national security.

Because these debates will involve a good deal more than national security, they will often be settled on other than national security grounds, at least where the pure national security issue is a close one, as debatable issues tend to be in a more and more complicated world. Constraints, therefore, are more and more important, and there are several kinds of constraints that can be expected to press a good deal harder on the decisionmaking process than they have in the past. These can be classified broadly as constraints based on resources, constraints based on dollars, and on balance of payments considerations, constraints based on political commitments, domestic and foreign, and constraints based on political repercussions, domestic and foreign.

Resource shortages over a wide range of resources and uses will clearly be a feature of the next quarter century. The list begins, of course, with energy shortages, which can impact both on national security objectives and on national security force structures and deployments. There is a good deal of debate about the nature and extent of other probable shortages in national resources, but there are at least indications that significant shortages of some such resources will appear from time to time. Meanwhile, awareness of environmental fragilities makes the exploration of available resources more difficult.

The last resource on the list, as predictably in short supply, is manpower, or rather military manpower. Shortages here result from the fact that, despite generally high levels of unemployment, voluntary recruitment for the military is likely to have a high marginal cost. When the decline in the number of births hits the age cohort for entrance to military service, about 1985, the problem will become more serious, particularly in the reserve components. Since compulsory service probably cannot be reinstated, absent a major international crisis, the high cost of military manpower may limit both the overall size of the armed forces and the amount that can be spared for new or improved weapons systems.

Perhaps the most direct way to moderate this constraint would be to expand greatly the proportion of women in the armed services, substituting person power for manpower alone. Another complementary approach would be to initiate a major program of voluntary national service, creating a context in which non-career voluntary military service could be seen as a form of national service for which one would receive a minimal stipend, rather than a paycheck competitive with the private sector.

The supply of military officers qualified to deal with the increasingly complex problems of national security may not be a constraint on the policy process, but only if even more vigorous efforts are made to prepare senior officers for their roles in the civil-military dialogue. Samuel Huntington's classic distinction between "objective' and "subjective" civilian control of the military, that is to say between educating military leaders to understand and share the civilian point of view, or simply keeping military men out of civilian matters, has already been resolved by events in favor of the former approach. There remains some uncertainty about how best to implement that approach — through changes in the military educational system, through greater ease of movement back and forth between the military and the civilian sectors, with concomitant modifications in the military retirement scheme, and through more exchanges between military and civilians like the ones embodied in this conference. In my own experience, military professionals are at least as responsive to civilian leadership as any other professional group in public service, but the tasks are becoming more challenging, and the preparation must continue to meet the challenges.

Even with a new kind of voluntary (enlisted) military service, dollar constraints on national security budgets and force structures will become, if anything, more serious. The problem arises because relatively so small a proportion of the federal budget is discretionary spending, and political reluctance to increase taxes is increasing. Whatever tax dividend might result from a slowly rising GNP is likely to be consumed in the rising cost of existing federally-supported social services. Whether or not the national

security budget is an appropriate target for budget cutters, it is one of the few targets in sight.

Direct budgetary concerns are exacerbated by the fact that a portion of military spending involves balance-of-payments costs as well. Some of those costs can be offset, but the use of arms sales agreement to offset balance-of-payments costs has managed to create more problems than it has resolved, and will probably not be available as a policy instrument in this context.

The web of political commitments in which government involves itself is a function both of the increasing politicization of the economic structure, and of the increasing interdependence of the world we live in. Government is constantly making promises to domestic interest groups, and to allies and friends abroad. Domestic promises may be broken, but at a substantial cost in present good will and future trust. We are a good deal more reluctant to make international promises today than we have been over the past 20 to 25 years. But this gives greater significance to the promises we do make. To abrogate or to repudiate them is to threaten international stability.

Even where government does not promise, it is extremely reluctant to undertake any actions that will have adverse repercussions on any organized interest group. And adverse reprecussions will be more frequent in a more tightly-knit, interdependent world. The power of veto groups over national policy is thus substantially enhanced. For example, the military force structure may be sized and shaped on the basis of certain assumptions about the degree of energy independence to be achieved in the United States. But that energy policy objective may have to be significantly modified as a result of objections from the auto industry (and the UAW) even in the absence of any commitments by the government to those interest groups. Similarly, in thinking about military deployments around the world, we need to consider not only the reactions of our potential adversaries, but those of other nations and groups of nations, great and small, allies and friend, and "nonaligned" states.

There is a fifth kind of constraint that needs to be considered here as well, and that is the availability of suitable forums for debate and discussion of national security issues, and, at least equally important, the interest of the general public in participating, even as observers, in those forums.

We begin with an enormous range of activities, from courses in high schools, colleges and universities, and articles in learned journals to television documentary "specials" on national security issues, and institutional advertisements in newspapers and magazines. These activities can be arranged on a number of scales: size of audience, degree of audience participation, degree of audience interest (probably closely correlated), depth of exploration of the issues, partisanship, breadth of exposure to a wide range of viewpoints, degree of (perceived) influence of the forum on the actual outcome, etc.

It may be useful to distinguish, at the outset, between maintenance and expansion of the general knowledge base on national security matters, and exploration of particular current issues. By and large, American society seems to be doing better with the second task than with the first.

Immediately after World War II, the educational community responded to the new role of the United States in the world with new attention to teaching and research on national security topics. The phenomenon of Sputnik increased that attention, and multiplied the resources made available, from public sources, through the National Defense Education Act of 1958 and related legislation, and from private sources, primarily through the great foundations. These resources had their intended multiplier effect, in the decisions of school boards and college and university faculties about new courses, in the decisions of students about choice of courses, and of scholarly careers, and in the research orientation of private research organizations. Language and area studies programs sprang up everywhere, as did national security studies programs on a smaller scale. Permanent federal legislation was even proposed to finance graduate study and research.

But the federal legislation was never enacted, although the foundations, anticipating its enactment, cut back their support in the field. Newly created programs, not yet established within the core budgets of colleges and universities, found themselves struggling for a share of an increasingly limited pool of outside resources. And as educational institutions, at all levels, moved from the fat years to the lean years, the financial problems of national security teaching and research became even more acute. In higher education, even more than in most bureaucracies (using the word in no invidious sense) seniority is critical in the distribution of resources, and in a period of contraction it is the most recently-established programs that are likely to suffer the most.

One exception to this reversal of trend has been the research institutions supported by the military itself — Rand, CNA, RAC — but they are necessarily concerned more with the elucidation of current problems than with maintenance of the general knowledge base.

At the same time there has been a proliferation of private institutions addressing current national security issues: examples include the Hudson Institute (established in 1962) and the Institute for Strategic Studies (now the International Institute for Strategic Studies) established in 1958, the Center for Strategic Studies

and the Defense Information Center, the Center for Strategic and International Studies at Georgetown, and the Center for National Security Studies. The Brookings Institution set up a Defense Policy Study Group, and Harvard University organized a program for Science and International Affairs, while Harvard, MIT, Cornell, and Stanford have joined a coalition, the Arms Control Consortium, organized under the auspices of the Aspen Institute. This last group of activities, although conducted within the university framework, is distinguishable from the first category of programs in that they have tended to find support outside the university itself and have consequently focused their attention more on current issues and problems.

If this combination of trends continues, it suggests a danger that there may be more serious but basically less well-informed interest generated in national security issues — or even that the proponents of particular points of view may find themselves more and more either preaching to the converted, or engaging in a dialogue of the deaf.

There is, however, a counter-tendency to incorporate the international aspects of any academic subject — from anthropology to zoology — directly into the study of that subject. This seems a natural development as the world becomes more interdependent, and it naturally incorporates national security issues as well. Yet the inclusion of this material is not an adequate substitute for the availability of courses focused directly on foreign policy and national security issues, any more than scholars in anthropology or zoology would be satisfied to have their disciplines incorporated into the study of foreign policy.

The same considerations that apply to the development of academic disciplines apply to the presentation of public issues in the media. It is more and more difficult for even the most parochial to ignore the international and national security aspects even of the local news. But the treatment of international issues is so casual and compressed even in the print media — and even more so in the broadcast media — that it scarcely provides a basis for intelligent citizen judgments. Journalists who cover national security news are too often lacking in substantive background and expertise in the subject matter — although there are notable exceptions. And the information scarcity problem is exacerbated because while citizens can supplement what they learn from the media about local issues through word of mouth and actual firsthand exposure, there is very little opportunity to supplement their information about foreign affairs, and what supplementary information is available is likely to be quite limited by accidents of time and place.

If current information on national security issues is becoming more widely available, a question then arises as to the interest of the general public in that information, and in the debates on national security policy that are (one hopes) based on that information. I have argued above that there is a wider range of special interests involved in the new kind of national security issues. There is nothing sinister or even improper in the involvement of these interests. But national security policy ought to be more than the resultant of all the lines of force that they exert. Unless there is significant interest and concern on the part of the general public, the main line of national security policy may be discontinuous, and erratic — a series of zigs and zags to which the observer cannot fit a regular curve.

Recent events — Watergate and its attendant revelations, the last act of Vietnam, and the violent death of three national leaders — have all tended to alienate Americans from our government. Although the peaceful transition from these unhappy events has demonstrated the strength of our democracy, it has left many citizens with a pervasive and persistent sense of powerlessness. Paradoxically, the new campaign finance laws have contributed in a way to this sense, at least temporarily, by cutting off a traditional avenue of citizen involvement — fund raising — in Presidential elections. If, however, campaign contributions are severely limited in amount but still permitted by future campaign financing laws, the net effect may be to reduce the sense of nonparticipation.

Unless and until that sense is overborne by an appreciation of the opportunities for participation in policymaking, citizens whose primary concern is with the public interest will not be drawn into the policymaking process. There are some indications of a resurgence of this kind of concern, not yet on anything like the scale that it manifested itself when the Marshall Plan was proposed, or at the height of the Vietnam debate. The key to citizen interest is probably to be found in Presidential leadership; that is one of the principal tasks that President Carter has set for himself, and, as he has put it in another context, he intends to succeed.

PARTICIPANTS

Chairman

Honorable Brent Scowcroft, Lieutenant General, USAF (Ret.)

Authors

Professor Robert S. Wood, Department of Government and Foreign Affairs, University of Virginia

Professor Adam Yarmolinsky, University of Massachusetts, Downtown Center

Panelists

Mr. E. C. Aldridge, Systems Planning Corporation

Dr. Roy Amara, President, Institute for the Future

Mr. Ronald H. Brown, Deputy Executive Director, National Urban League

Honorable William E. Colby, Former Director, Central Intelligence Agency

Honorable Leslie Gelb, Director, Bureau of Politico-Military Affairs, Department of State

General Harold K. Johnson, USA (Ret.), Financial General Corporation

Mr. Crosby Kelly, Vice President, Rockwell International Corporation

Mr. John H. Lyons, President, Ironworkers International

Dr. Earle C. Ravenal, Georgetown School of Foreign Service

Ms. Joyce Lasky Shub, Foreign Policy Advisor to Senator Biden

LTGEN William Y. Smith, Assistant to the Chairman, The Joint Chiefs of Staff

General Maxwell D. Taylor (Ret.)

MG Jasper A. Welch, USAF, Assistant Chief of Staff (Studies and Analysis), United States Air Force

Rapporteur

LTC Thomas A. Pianka, USA